

HHS Privacy Impact Assessment (PIA) Summary

CMS: Administrative Finance Systems

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

2Summary of PIA Required Questions

Question

Response

1 System:	Administrative Finance Systems
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-01-04-01-1090-00 009-38-01-01-01-1020-00
7 Privacy Act System of Records (SOR) Number:	09-90-0024
8 OMB Information Collection Approval Number:	N/A
9 Other Identifying Number(s):	N/A
10 System Name:	Administrative Finance System
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	Antoinette Miller
12 Provide an overview of the system:	<p>ATARS: Track the process of an OIG or GAO audit through CMS clearance process, then monitor the monies collected, saved, or written off.</p> <p>BAAADS: Provides the OFM/FSG administrative budget staff the capability to disperse funding to CMS components. Funding is allocated at the appropriate level and components are notified of their funded amount via an advice of allotment/allowance. BAAADS is interfaced with FACS to provide for funding input and modifications.</p> <p>BUCS: Agency-wide budget execution system used by Executive Officers and their staff to manage and track administrative funds.</p> <p>DCS: Allows CMS employees to enter, update, and transmit overpayment debt for the purpose of collecting debt through Treasury offset.</p> <p>FACS: Accounting, general ledger, and payment functions.</p> <p>HTS: Allows CMS employees to enter, submit, and approve travel documents for the purpose of receiving reimbursement of travel expenses.</p>
13 Indicate if the system is new or an existing one being modified:	Existing
14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	Yes
15 Is the system subject to the Privacy Act?	Yes
16 If the system shares or discloses IIF please specify with whom and for what purpose(s):	ATARS: N/A BAAADS: N/A BUCS: N/A DCS: N/A FACS: Delinquent receivables sent to HHS/PSC’s Debt Referral System (DMCS). PSC sends data to Treasury Offset Program (TOPS). Payment files sent to Treasury. 1099-Misc. files sent to IRS. Budget data extracted from a FACS report file by the BUCS. HTS: N/A

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: Administrative Finance Systems

- 17

Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:
- ATARS: The information CMS collects is OIG or GAO audit information. It will be used for tracking purposes. It does not contain IIF.

BAAADS: The information CMS collects is from the Office of Management and Budget based on the Congressional appropriation. It does not contain IIF.

BUCS: CMS Administrative budget data is collected and maintained in BUCS. Funding records contain CMS accounting information including Allowance Number and Common Account Number, Administrative organization codes and funding data. Spending records are detailed budget transactions and contain name, transaction description, dates, spending amounts, object class, CAN and budget identifying codes. Information contains IIF, and submission is mandatory.

DCS: Information associated with principal and interest and individual debtors whether they are individual or corporations. Information contains IIF, and submission is mandatory.

FACS: The IIF contained in the FACS includes vendor and employee EINs/TINs, names, addresses, and banking information. Submission of this information is mandatory, as it is required to make payments to vendors and individuals. Information on taxable payments is sent to the Internal Revenue Service. Additionally, this information must also be tracked for receivables, as this information will be used when referring delinquent debts to the Treasury for collection.

HTS: Information associated with an employee and travel expenses are collected. The information contains IIF, is mandatory for employees to receive reimbursement of valid travel expenses.
- 18

Describe the consent process:
- ATARS: NO.

BAAADS: NO

BUCS: The SSN is only used to systematically retrieve a name on a transaction. When a name is added to a transaction, it is selected from a transaction drop down list that only displays the name of CMS Employees from a reference table. The reference table is maintained by the BUCS technical administrator and is not available to BUCS users.

DCS: The IIF information is supplied by individuals and corporations.

FACS: IIF is obtained from vendors and employees, who are instructed that this information is required in order to receive payment from the CMS. This is conveyed to them through contract and/or appropriate CMS notification (when they are being reimbursed for travel). Vendors can not sign their contract, and employees can not be reimbursed for travel if they do not want to provide this information to the CMS.

HTS: The IIF information is supplied by the personnel file.
- 19

Does the system host a website?
- No
- 20

Does the website have any information or pages directed at children under the age of thirteen?
- No
- 21

Are there policies or guidelines in place with regard to the retention and destruction of IIF?
- Yes
- 22

Are there technical controls present?
- Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Administrative Finance Systems

- 23 Describe the IIF security controls:

ATARS:No

BAAADS: No

BUCS: The data is secured by Oracle database security rules and constraints. User authority is granted via the establishment of user ids and database authorities. In addition, BUCS maintains and controls application security by the establishment of user profiles and specific table access authority.

DCS: The data is secured by DB2 database security rules and constraints. User authority is established via a userid/password.

FACS: IIF is secured through CMS data center policy, as well as the secure CMS facility. Additionally, user-level security includes RACF security, user classes within the FACS, security groups limiting access based on dataset high-qualifiers and usage requirements, and screen-level security.

HTS: The data is secured by Oracle database security rules and constraints. User authority is established via a userid/password.
- 24 Sr Official of Privacy Signature:

Abby Block
- 25 Sr Official of Privacy Signoff Date:

Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: CMS IT Infrastructure IS

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer "No" to that question.

2 Summary of PIA Required Questions

Question	Response
1 System:	CMS IT Infrastructure IS
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-01-04-01-1160-00 009-38-01-09-01-1120-00 009-38-02-00-01-1150-00
7 Privacy Act System of Records (SOR) Number:	09-70-0064
8 OMB Information Collection Approval Number:	N/A
9 Other Identifying Number(s):	N/A
10 System Name:	CMS IT Infrastructure
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	Charlene Fletcher
12 Provide an overview of the system:	<p>As a part os the Medicare Modernization Initiative, CMS is changing the way that is does its Medicare claims business. The Medicare Administrative Contracts are being awarded to migrate the traditional fee-for-service Title XVIII contracts over to Federal Acquisition Regulation contracts. Additionally, CMS is taking ownership of the data processing portion of this business its award of the Enterprise Data Center (EDC) contract in March 10, 2006. This contract will migrate the workloads and MEDicare Claims processing systems that are currently running at 14 Medicare data centers in different physical locations to one of the three EDC contractors, (CDS' Cloumbia SC Data Center, EDS' Tulsa Chrokee Data Center and IBM's Southbury Data Center.)</p> <p>Additionally, this site now supports CMS' web hosting application, (e.g., Medicare.gov, cms.hhs.gov. and HPMS). This GSS does not directly collect, maintain, or disseminate information. It provides platform support infrastructure for other CMS MA's to performm their function.</p> <p>Part A Shared System: Hospital insurance claims process through the Fiscal Intermediaries Shared System, which performs claims processing and benefit payment functions for institutional providers under Parts A and B of the program.</p> <p>Part B Shared System: The PArt B Shared System supports the processing of Medicare Part B claims, Medicare Part B is supplemental medical insurance, which covers physician services and other outpatient services. The Shared System for Part B Medicare in the Multi Carrier System. Medicare Part B claims processing contractors are known as Carriers, and include the Railroad Retirement Board. They process physician and supplier claims provided under MEDicare Part B coverage.</p> <p>Durable Medicare Equipment Regional Contractor Shared Syste: CMS has designated four carriers to have exclusive responsibility for handling Medicare Part B claims, for Durable Medicare Equipment Prosthetics, Orthotics, and Supplies claims in specific geographic regions of the United States. They are commonly referred to as the DMERCs. The selected DMERCs currently use the VMS DME Shared system to process DMEPOS claims. This GSS provides compute platforms, telecommunications, electronic storage infrastructure, and operations support services for the collection, maintenance, and access of data and information to support the business functions of CMS.</p>
13 Indicate if the system is new or an existing one being modified:	Existing

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

## CMS: CMS IT Infrastructure IS

- 14

Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?
- Yes
- 15

Is the system subject to the Privacy Act?
- Yes
- 16

If the system shares or discloses IIF please specify with whom and for what purpose(s):
- The agency may share the collected information with a variety of Federal, state, local and tribal government audiences and professional audiences, including the medical community. This includes, Providers, Ambulance Services, Medigap Companies/Supplemental Insurers, Clinical Labs, CMS contractors, DME Suppliers, Health Plans, Hospitals, Home Health Agencies, Physicians, Potential Contractors, Researchers, Skilled Nursing Facilities, and Suppliers.
- 17

Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:
- This information is used to process claims and payments for the MEDicare Program beneficiaries. Submission of this information is mandatory and includes IIF. The agency through MEDicare contractors and beneficiaries collects information through CMS forms CMS-1450 and CMS-1500. These are OMB approved forms. Information is collected primarily through electronic means.
- 18

Describe the consent process:
- Information is collected from two CMS forms, the 1450 and 1500. All Medicare Claims Processing Contractors are called 'satellites' under CWF. Satellites access the HOST CWF databases to obtain needed beneficiary information. Satellites submit claims to the CWF Host for prepayment review and approval. Medicare beneficiaries are provided healthcare services where their personal information is collected and required for payment and reimbursement purposes. Beneficiaries receive HIPAA disclosure information by providers and Medicare directly. A complaint process is in place for individuals to raise their privacy concerns.
- 19

Does the system host a website?
- Yes
- 20

Does the website have any information or pages directed at children under the age of thirteen?
- No
- 21

Are there policies or guidelines in place with regard to the retention and destruction of IIF?
- Yes
- 22

Are there technical controls present?
- Yes
- 23

Describe the IIF security controls:
- The Medicare Claims Processing Systems incorporate a variety of security measures to protect IIF. These include physical, administrative, and technical.
- 24

Sr Official of Privacy Signature:
- Abby Block
- 25

Sr Official of Privacy Signoff Date:
- Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

CMS: CMS Security Program

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

2

## Summary of PIA Required Questions

Question	Response
1 System:	CMS Security Program
2 Is this a new PIA?	-
3 If this is an existing PIA, please provide a reason for revision:	-
4 Date of this Submission:	-
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	-
7 Privacy Act System of Records (SOR) Number:	-
8 OMB Information Collection Approval Number:	-
9 Other Identifying Number(s):	-
10 System Name:	-
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	-
12 Provide an overview of the system:	-
13 Indicate if the system is new or an existing one being modified:	-
14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	-
15 Is the system subject to the Privacy Act?	-
16 If the system shares or discloses IIF please specify with whom and for what purpose(s):	-
17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:	-
18 Describe the consent process:	-
19 Does the system host a website?	-
20 Does the website have any information or pages directed at children under the age of thirteen?	-
21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?	-
22 Are there technical controls present?	-
23 Describe the IIF security controls:	-
24 Sr Official of Privacy Signature:	-
25 Sr Official of Privacy Signoff Date:	-

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



HHS Privacy Impact Assessment (PIA) Summary

CMS: Customer Service Systems

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer "No" to that question.

2Summary of PIA Required Questions

Question	Response
1 System:	Customer Service Systems
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-01-09-01-1020-00 009-38-01-04-01-1060-00
7 Privacy Act System of Records (SOR) Number:	09-70-0533, 09-70-0544, 09-70-0535, 09-70-4004, 09-70-0516, 09-70-0513, 09-70-0542, 09-70-0566
8 OMB Information Collection Approval Number:	N/A
9 Other Identifying Number(s):	N/A
10 System Name:	Customer Service System
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	1. Greg Overland & Jon Booth, 2. Tim Walsh, 3. Dave Nelson, 4. Macia Thorpe-Johnson, 5. Timothy P Wlash & Ketan Patel
12 Provide an overview of the system:	1. cms.hhs.gov is the official public Agency website of the Centers for Medicare & Medicaid Services, accessible at www.cms.hhs.gov. The cms.hhs.gov website was launched on September 13, 2001. This site was a replacement for the Agency's prior website, www.hcfa.gov. The Health Care Financing Administration launched the hcfa.gov website in 1995. While the cms.hhs.gov contained much of the same content as hcfa.gov, it did feature a new design and organization scheme. 2. The MBP provides Medicare beneficiaries with a browser-based graphical user interface (GUI) to retrieve relevant beneficiary information. 3. The NGD and MyMedicare.gov is a customer relationship management system. The NGD desktop was developed to handle inquiries for the 1-800 Medicare Helpline and Medicare Intermediary Contracotrs. The NGD was designed to support the VCS initiatives of the DCCO. The MyMedicare.gov is a web interface available to the Medicare Community. 4. The BCC serves citizens nationwide by accepting and responding to inquiries relating to Medicare and MEDicaid benefits and other related services through HHS, CMS. Support services provided by the BCC include: responding to telephone inquiries using scripted and plain language, escalating calls as needed; answering e-mail and written correspondence; maintaining and delivering a training program; fulfilling static and print-on-demand publication requests; installing and maintaining telecommunications networks and network-based applications; employing Intelligent Call Routing for call delivery. 5. The applications that comprise CMS's Customer Service Systems - Medicare.gov Website enable the Agency to educate the public, specifically Medicare beneficiaries, on the Medicare program. Originally launched in 1998, Medicare.gov allows consumers to compare health plans, nursing homes, home health agencies, prescription drug coverage, and participating physicians.
13 Indicate if the system is new or an existing one being modified:	Existing
14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	Yes
15 Is the system subject to the Privacy Act?	Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Customer Service Systems

- 16

If the system shares or discloses IIF please specify with whom and for what purpose(s):
- 17

Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:
1.

Information is shared with the appropriate staff within the agency. Subject matter experts are asked to respond to inquiries in their field of knowledge.
2.

Beneficiaries for the purpose of providing self service to data available via the call center
3.

SSA Order Medicare Cords, SSA Medicare, MARx System; Vangent, CGI Federal, Palmetto GBA for user acceptance testing; data also recorded in NGD is also used to populate personal data in the National Data Warehouse
4.

Vangent will share IIF with CMS and subcontractors to perform under Business Associate Agreement
5.

Posted on website for informational purposes
1.

Data is collected to: improve the Agency's website; allow visitors to ask specific questions of Agency staff; and support conference registration for outreach and educational purposes. At all data collection points, a link to the website privacy policy is provided (the privacy policy is linked from the website footer so that it is available on all pages). When a user submits feedback they get a response explaining how their data will be used. Similarly, conference registrants receive an email confirmation explaining the use of their data. Information is collected at several points in the site. Specifically, users can submit feedback and questions through our "Feedback" link. The only data element explicitly requested is an email adress. This is a voluntary submission. These feedback requests are triaged automatically to the appropriate business component for response. Additionally, we have an online conference registration system available. This system captures contact information from registrants, including, name, business, adress, phone, fax and email. This information submission is voluntary and is automatically sent to the conference coordinator and removed from the website after 60 days.
2.

The MBP will collect Beneficiary Login Information (medicare number and password) for identification and authentication purposes. For registration, the mBP will collect the user's Medicare Number, last anme, date of birth, gender and zip code for identification. A user cannot register without providing this information. Once registered, the user can access the application via their username and password.
3.

The NGD and My.Medicare.gov collects and stores information about Medicare beneficiaries. Access to beneficiary Medicare information requires callers and users of my.medicare.gov to submit identifying information. The Health Insurance Claim Number is utilized as required to identify information about the beneficiary and validated with additional IIF information such as Beneficiary Name, address, date of birth, etc. The purpose of the information collected, maintained, and disseminated is to answer Medicare beneficiary inquiries.
4.

The information collected, maintained, or disseminated contains IIF. Submission is voluntary. Information includes Privacy Act data elements which are used to access and provide information being requested by Medicare beneficiaries.
5.

Information collected from users of Medicare.gov is collected during Publications Ordering. The only required data elements collected are user name (first and last) and address. Other information collected from users of Medicare.gov is in the form of voluntary feedback, which can be submitted via the "Questions" or "Feedback" links. The only data element explicitly requested is an email address.

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Customer Service Systems

- 18 Describe the consent process:

1. None in place

2. The MyMedicare.gov usage is managed through SSL secure connections. The usage of MyMedicare.gov is managed through confidential communication with the Medicare beneficiary. IIF information is shared on a need to know basis at the direction of CMS.

3. The users of the NGD are required to use HIPAA compliant disclosure procedures before disclosing any IIF information about a Medicare beneficiary. The NGD tracks disclosure activities of the customer service representative. The NGD will provide Medicare related general, eligibility and claim information to the Medicare beneficiaries in the form of phone calls and written requests.

4. Not Applicable

5. At all data collection points, a link to the website privacy policy is provided. The policy indicates that CMS will protect the personal information that the user shares with us and that CMS does not disclose, give, sell, or transfer and personal information to third parties. Information collected from users of Medicare.gov is collected during the Publications Ordering. The only required data elements collected are user name (first and last) and adress. Other information collected from users of Medicare.gov is in the form of voluntary feedback, which can be submitted via the "Questions" or "Feedback" links. The only data element explicitly requested is an email address.
- 19 Does the system host a website?

Yes
- 20 Does the website have any information or pages directed at children under the age of thirteen?

No
- 21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?

Yes
- 22 Are there technical controls present?

Yes
- 23 Describe the IIF security controls:

1. All IIF is secured behind user lds and passwords. IIF collected through the website is not publicly accessible. In addition, the conference registration application, which collects more IIF than the user feedback, is secured by SLL encryption.

2. The MBP system is designed to secure information while in transit on the network. When user information is in transit on the network. When user information is in transit, the MBP system uses encryption to provide data confidentiality.

3. The NGD and MyMedicare.gov system secures IIF by implementing a multi-tiered architecture using multiple types and layers of firewall and intrusion detection technology. The Siebel infrastructure allows for strict role based user access controll that restricts access on both. NGS policies require management authorization of all access to data and data processing systems as well as physical access. All access is based on the principle of "Need to KNow". Physical controls include ID badges, key cards, cipher locks, and cloased circuit tv (CCTV). Access to the data center is strictly controlled and requires additional approval by the Data Center Manager. The access control list and visitor logs are reviewed on a monthly basis by the Data Center Manager.

4. Vangent has internal controls to protect the confidentiality, integrity, and availability of IIF using existing administrative, technical and physical controls including Standard Operating PROcedures for Business Continuity and Disaster Recovery; Environmental Safeguards; Operating systems/application/network level logging, physical and logical identification and autherntication, Intrusion Prevention Systems; firewalls, virtual private Networks, Guards and CCTV.

5. All IIF is secured behind userlds and passwords. IIF collected through the website is not publicly accessible. In addition, the publications ordering application, which collects more IIF than the user feedback, is secured by SSL encryption.
- 24 Sr Official of Privacy Signature:

Abby Block
- 25 Sr Official of Privacy Signoff Date:

Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

CMS: Health Care Quality Improvement Systems

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

2

## Summary of PIA Required Questions

### Question

### Response

- 1

System:
- Health Care Quality Improvement Systems
- 2

Is this a new PIA?
- No
- 3

If this is an existing PIA, please provide a reason for revision:
- PIA Validation
- 4

Date of this Submission:
- Jun 29, 2007
- 5

OPDIV Name:
- CMS
- 6

Unique Project Identifier (UPI) Number:
- 009-38-01-06-01-1030-00 009-38-01-06-01-1010-00
- 7

Privacy Act System of Records (SOR) Number:
- 09-70-9002, 09-70-0525, 09-70-0521, 09-70-0565, 09-70-0520, 09-70-0531, 09-70-0543, 09-70-0591, 09-70-0574, 09-70-0547, 09-70-0519, 09-70-0069
- 8

OMB Information Collection Approval Number:
- 0938-0581
- 9

Other Identifying Number(s):
- N/A
- 10

System Name:
- Health Care Quality Improvement System
- 11

System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:
- Dennis Stricker

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: Health Care Quality Improvement Systems

- 12

Provide an overview of the system:
- The Consolidated Renal Operations in a Web-enabled Network (CROWN) will facilitate the collection and maintenance of information about the Medicare End Stage Renal Disease (ESRD) program.

CROWN is being developed to modernize the collection and retrieval of ESRD data in a secure, Web-enabled environment. The new capabilities will allow dialysis facilities to enter information electronically and transmit it to the appropriate ESRD Network, and CMS also will be able to send feedback to the Networks and the facilities through the new environment. CROWN consists of the following major modules:

The Vital Information System to Improve Outcomes in Nephrology (VISION), which will support electronic data entry and encrypted transmission of ESRD patient and facility data from dialysis facilities. The ESRD Standard Information Management System (SIMS) supports the business processes of the ESRD Network Organizations.

The Renal Management Information System (REMIS) which determines the Medicare coverage periods for ESRD patients and serves as the primary mechanism to store and access ESRD patient and facility information.

The ESRD Program was established in 1972 pursuant to the provisions of 299I, Public Law 92–603. Notice of this system, ESRD/PMMIS was published in a Federal Register at 53 FR 62792 (Dec. 29, 1988), 61 FR 6645 (Feb. 21, 1996) (added unnumbered SSA use), 63 FR 38414 (July 16, 1998) (added three fraud and abuse uses), and 65 FR 50552 (Aug. 18, 2000) (deleted one and modified two fraud and abuse uses).

The Standard Data Processing System (SDPS) consists of many data and reporting requirements and was designed and developed in response to the ongoing information requirements of the Quality Improvement Organizations (QIOs) and other affiliated partners, such as the Clinical Data Abstraction Centers (CDACs) to fulfill their contractual requirements with CMS. This system, which became operational in May 1997, interfaces with CMS Central Office, 53 QIOs and CDACs.

This legislation is under Title XI of the Social Security Act, Part B, as amended by the Peer Review Improvement Act of 1982.

QIES encompasses systems that provide data collection, management reporting, provider feedback and national warehousing. QIES is divided into four primary areas: Assessment management report feedback; Quality Indicator/Quality measure surveillance and feedback; and the National QIES repository and CASPER reporting system.
- 13

Indicate if the system is new or an existing one being modified:
- Existing
- 14

Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?
- Yes
- 15

Is the system subject to the Privacy Act?
- Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

CMS: Health Care Quality Improvement Systems

16	<p>If the system shares or discloses IIF please specify with whom and for what purpose(s):</p>	<p>Consolidated Renal Operations in a Web-Enabled Environment (CROWN) is a Major Application (MA) whose purpose is to facilitate the collection and maintenance of information about the Medicare ESRD program, its beneficiaries, and the services provided to beneficiaries. The major CROWN applications provide support for CMS organizational business processes by conducting activities that meet the following CMS goals for the ESRD program:</p> <p>Improve the quality of health care service and quality of life for ESRD beneficiaries; Improve data reliability, validity, and reporting among ESRD providers/facilities, Networks and CMS (or other appropriate agency). Establish and improve partnerships and cooperative activities among and between the ESRD Networks, Quality Improvements Organization (QIOs), State survey agencies, ESRD providers/facilities, ESRD facility owners, professional groups, and patient organizations.</p> <p>Each participating ESRD facility and network will be required to have a workstation with a minimum system configuration as specified by QualityNet Exchange. QualityNet Exchange will provide the ability for ESRD Networks to securely exchange multiple types of data files such as MSWord, Excel, Text, and PowerPoint, in real-time via the Internet. These files could be used for letters, static reports, comparative clinical data, and general information.</p> <p>Additionally, QualityNet Exchange will provide an interactive, secure web site that will allow End Stage Renal Disease (ESRD) Facilities to transmit electronic patient data to their corresponding ESRD Network. ESRD Networks will use the QualityNet Exchange to transmit "seed" patient databases to Facilities, receive electronic patient data files from Facilities, and provide feedback to Facilities regarding data transmission. QualityNet Exchange will be responsible for routing files to/from the appropriate ESRD Facilities and Networks and ensuring that each Facility and Network can only access their data files.</p> <p>REMIS will allow users to view ESRD beneficiary and provider information from the eighteen ESRD Network organizations housed in the Standard Information Management System (SIMS) Central Repository.</p> <p>Internal users:</p> <ul style="list-style-type: none"><li>· ESRD Networks</li><li>· CMS OCSQ staff (i.e., the Analysts)</li><li>· Application Administrators (i.e., Supervisors, etc.)</li><li>· System Administrators (i.e., DBA's)</li><li>· Other CMS users (i.e., Actuaries)</li><li>· Developers (i.e., Programmers).</li></ul> <p>External users:</p> <ul style="list-style-type: none"><li>· ESRD Facilities</li><li>· National Institutes of Health (NIH)</li><li>· Health Insurance Companies (Medicare Secondary Payers)</li></ul> <p>Users of the SDPS data systems include: CMS Central and Regional offices, QIOs, Medicare certified inpatient providers, and authorized PMS vendors.</p> <p>Any 'sharing' of this information outside of the group mentioned above can only be approved by CMS. A Data Use Agreement is submitted to CMS for approval.</p> <p>The Standard Data Processing System (SDPS) is a Major Application (MA) whose purpose is to provide hardware and software tools to enable Quality Improvement Organization personnel to fulfill the</p>
----	--	--

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Health Care Quality Improvement Systems

requirements of the QIO programs. The primary purpose of the system is to aid in the administration and monitoring of the tasks mandated by the QIO program. These tasks include:

- Improving Beneficiary Safety and Health Through Clinical Quality Improvement in provider settings of: a. Nursing Home; b. Home Health; c. Hospital; d. Physician Office; e. Underserved and Rural Beneficiaries; and f. Medicare + Choice Organizations (M+COs).
- Improving Beneficiary Safety and Health Through Information and Communications by: a. Promoting the Use of Performance Data; b. Transitioning to Hospital-Generated Data; and c. Other Mandated Communications Activities.
- Improving Beneficiary Safety and Health Through Medicare Beneficiary Protection Activities through: a. Beneficiary Complaint Res

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

CMS: Health Care Quality Improvement Systems

17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:

The Consolidated Renal Operations in a Web-enabled Network (CROWN) will facilitate the collection and maintenance of information about the Medicare End Stage Renal Disease (ESRD) program, as follows:

VISION provides an electronic data entry and reporting system for the nearly 4000-dialysis facilities in the United States. The information stored in VISION is collected by the ESRD dialysis facility or transplant unit and submitted to the ESRD Networks via Quality Net Exchange. The data collected via the VISION tool is mostly patient registry data to track the patients through their dialysis treatments and transplants. The VISION system also collects some Quality Improvement data via the Clinical Performance Measures tool that will be rolled out this spring. Currently, there are about 135 facilities out of 4600 facilities nationally that are using this system.

Data from VISION is uploaded via Quality Net Exchange to the ESRD Networks. The ESRD Networks import this data into their local SIMS System and perform additional validation and edit checks on the integrity of the data. SIMS, in addition to the patient registry data, also houses clinical data such as vascular access information, and in the near future, electronic laboratory data. Currently, SIMS is used by all employees at every ESRD Network to which all 4600 dialysis facilities and transplant facilities report.

SIMS focuses on the mission critical operations of the ESRD Networks. These operations have been categorized into 5 major areas.

- Form Entry/Submission and Tracking
- Reporting
- Administration
- Database Utilities
- Other SIMS Features

The REMIS (Renal Management Information System) is a web-based interactive database of ESRD patient and provider information located at CMS Data Center in Baltimore, MD. It is used by CMS and the renal community to perform their duties and responsibilities in monitoring Medicare status, transplant activities, dialysis activities, and Medicare utilization (inpatient and physician supplier bills) of ESRD patients and their Medicare providers. REMIS provides a central database for CMS ESRD information.

REMIS will support and improve data collection, validation, and analysis of the ESRD patient population over its predecessor system, REBUS. It will provide timely and accurate analysis information to the ESRD Network organizations, dialysis facilities, transplant centers, and research organizations. This will be accomplished via a Web-based data administration facility and decision support system. REMIS will provide improved support for ESRD program analysis, policy development, and epidemiological research.

REMIS will allow users to view ESRD beneficiary and provider information from the eighteen ESRD Network organizations housed in the Standard Information Management System (SIMS) Central Repository. The Networks provide Beneficiary, Provider, Medical Evidence, Death Notice, and Patient Event data. This information, along with information from CMS systems of record (Medicare Enrollment Data Base, the Common Working File, and the National Claims History, and from the United Network for Organ Sharing (UNOS), is integrated via REMIS.

The data that the SDPS system collects, maintains, and disseminates is as follows:

- summarized data for payment error rates by state and

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.





# HHS Privacy Impact Assessment (PIA) Summary

CMS: Health Care Quality Improvement Systems

nationally.

- claims,
- case review,
- medical record abstractions,
- payment information
- tracking of medical records,
- helpline and beneficiary complaint information
- raw and rolled up Part A and Part B claims
- tracking information for abstraction of surveillance data,
- beneficiary demographic information for all Medicare beneficiary enrollees,
- clearinghouse of information related to quality improvement information, tools, and techniques.
- 

- 18 Describe the consent process:
- CROWN: No  
SDPS: No  
QIES: No
- 19 Does the system host a website?
- Yes
- 20 Does the website have any information or pages directed at children under the age of thirteen?
- No
- 21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?
- Yes
- 22 Are there technical controls present?
- Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



23 Describe the IIF security controls:

CMS Information Systems Security Policy, Standards and Guidelines Handbook, Version 1.2, July 9, 2004, Chapter 16 establishes policy for the security of electronic mail, facsimile, and other media. It serves as the primary source of Information Technology (IT) systems security information for all CMS IT users. The policies, standards and guidelines described therein apply to all users of CMS hardware, software, information, and data. The CMS AIS Security Program ensures the existence of adequate safeguards to protect personal, proprietary, and other sensitive data in automated systems and ensures the physical protection of all CMS General Support Systems (GSSs) and Major Applications (MAs) that maintain and process sensitive data.

CMS QualityNet (QNet) System Security Policy Handbook, Version 3, April 24, 2006, Chapter 4 Guidelines for Destruction of Sensitive Information defines guidelines for the destruction of Medicare sensitive information and establishes a minimum set of security controls that will apply for all QualityNet users. These QualityNet guidelines will be used by the 3 QualityNet Complexes, 53 QIO sites responsible for each US state, territory, and the District of Columbia; 1 Clinical Data Abstraction Center (CDAC); and 18 End Stage Renal Disease networks.

These guidelines were established to provide a standard for QualityNet Functional Component users for the destruction of sensitive Medicare information. Users need to understand that taking personal responsibility for the handling, storage, and destruction of sensitive information is an essential part of their job.

This policy document meets the requirements set forth by the Computer Security Act of 1987 (P.L. 100-235), the Health Insurance Portability and Accountability Act of 1997 (P.L. 104-191), Appendix III to OMB Circular No. A-130 (50 FR 52730; December 24, 1985), and CMS Information Systems Security Policy, Standards and Guidelines Handbook, (The Handbook), Version 1.2, July 9, 2004.

The CROWN/ESRD information is secured in several different layers.

Physical layer - the hard copy data that comes into the ESRD Networks is secured at the local levels behind locked doors and is stored in locked file cabinets.

Hardware layer – All machines that store data have a login required, have an electronic screen saver password and all the application data is protected again behind a login to the software using a secure token.

Communication layer – the entire SIMS system relies on QualityNet (QNet) network infrastructure.

The SDPS system is a ‘closed’ system and consists of the following components:

Complex 1 located in the CMS Data Center in Baltimore, MD.  
Complex 2 located in the IFMC Data Center in West Des Moines, IA.  
Complex 3 located in Warrenton, VA.  
Development LAN and workstations at the IFMC SDPS complex;  
WAN connectivity between CMS Corporate and Regional Offices, QIOs, and AGNS. There is also connectivity to the IFMC SDPS complex.

The IFMC SDPS test and development servers are located in the IFMC corporate data center. The IFMC corporate data center is a restricted area and has appropriate environmental security controls implemented, to include measures to mitigate damage to Automated Information Systems caused by fire, electricity, water and climate changes. Access to the corporate data center is controlled by access cards, and only those with a business need to be in the data center are provided access via their access card.

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

CMS: Health Care Quality Improvement Systems

SDPS workstations and servers are also located at each of the QIOs. A QIO Manual was provided to each QIO when the original system was deployed. This document details the minimum requirements for environmental controls, electrical considerations, physical space and furnishings requirements, etc.

For access to all applications, users must complete a QNet Access Request Form, which has been automated for all but CMS RO users in the OARS system. This form specifies which system(s) the user Abby Block

Jun 29, 2007

- 24 Sr Official of Privacy Signature:
- 25 Sr Official of Privacy Signoff Date:

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Healthcare Integrated General Ledger Accounting System

1	
The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer "No" to that question.	
2	Summary of PIA Required Questions

Question	Response
1 System:	Healthcare Integrated General Ledger Accounting System
2 Is this a new PIA?	Yes
3 If this is an existing PIA, please provide a reason for revision:	-
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-01-01-1020-00-402-124
7 Privacy Act System of Records (SOR) Number:	09-70-0501, 09-70-0503, 09-90-0024
8 OMB Information Collection Approval Number:	N/A
9 Other Identifying Number(s):	N/A
10 System Name:	Healthcare Integrated General Ledger Accounting System (HIGLAS)
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	Janet Vogel
12 Provide an overview of the system:	To provide, in a production environment, a dual entry US Standard General Ledger accounting system and standardized accounting and financial management reporting process for CMS central office administrative program accounting activity and for the Medicare Program Benefits administered by the Medicare Fee-For-Service Claims Processing Contractors.
13 Indicate if the system is new or an existing one being modified:	New
14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	Yes
15 Is the system subject to the Privacy Act?	Yes
16 If the system shares or discloses IIF please specify with whom and for what purpose(s):	N/A
17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:	HIGLAS incorporates financial data that is focused on Medicare claims payment and overpayment collection activities. The main information maintained by HIGLAS is as follows: (1) Payables: supplier, bank, payment terms, location, BACS, UOM, employee receipt accrual, invoice, payment, remittance advice; (2) Receivables: customer, bank, payment term, BACS, UOM, item description, category, employee, invoice, receipt; (3) General Ledger/Budget Execution: set of books, BACS value, cross-validation rule, security rule, budget. The information is collected by the MEDicare Fee-For-Service Claims Processing Shared Systems which are SORs. These systems, in turn, populate HIGLAS with data needed to process payments to and collections from the Medicare fee-for-service payees.  Medicaid and SCHIP government award data: obligations, advances, and expenditures, grantee name, grantee EIN/TIN, CAN, and Object Class.
18 Describe the consent process:	HIGLAS does not collect IIF.
19 Does the system host a website?	No
20 Does the website have any information or pages directed at children under the age of thirteen?	No
21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?	Yes
22 Are there technical controls present?	Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Healthcare Integrated General Ledger Accounting System

- 23 Describe the IIF security controls:

HIGLA uses state-of-the-art technological methods to secure IIF. HIGLAS provides a much higher level of information security than previously available by meeting the following requirements for effective records security:
  - Ensures that only authorized personnel have access to electronic records
  - Ensures that appropriate agency personnel are trained to safeguard sensitive or classified electronic records
  - Ensures that appropriate contractor staff working as agents for the agency are trained to safeguard sensitive or classified electronic records
  - Minimizes the risk of unauthorized alteration or erasure of electronic records
  - Ensures that electronic records security is included in computer systems security plan prepared pursuant to the Computer Security Act of 1987, HIPAA of 1996, Privacy Act of 1974, OMB Circulars A-123, A-127 and A-130, Government Information Security Reform Act of 1996. JFMIP's Benefit System Requirements.
- 24 Sr Official of Privacy Signature:

Users have access only to the data required to perform their duties in the ORG to which they are assigned.
- 25 Sr Official of Privacy Signoff Date:

Abby Block  
Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

CMS: Human Resources Management Systems

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

2

## Summary of PIA Required Questions

Question	Response
1 System:	Human Resources Management Systems
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-02-00-01-1150-00
7 Privacy Act System of Records (SOR) Number:	09-70-3005
8 OMB Information Collection Approval Number:	No
9 Other Identifying Number(s):	No
10 System Name:	Human Resources Management Systems
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	Faraja Bryant-Ricketts, OOM/APSS, 410-786-2068

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Human Resources Management Systems

12	Provide an overview of the system:	<p>*10. Provide an overview of the system:</p> <p>CHRIS - The CMS Human Resources Information System is a portal for all CMS Human Resources and Personnel related data. This portal is a respository of information related to CMS employees. This portal is used by Human Resources and Management type personnel.</p> <p>ITSP-CBT – The 2002 FISMA requires all users of the Federal information systems to be exposed to security awareness materials at least annually. The ITSP-CBT provides CMS with the means to meet this requirement by providing basic information security awareness training to all individuals who have been issued a CMS USERID and have access to CMS information systems, to include but not limited to: CMS employees, contractors, students, guest researchers, visitors and others.</p> <p>FLSATRAV - The CMS FLSA Travel Tool allows CMS employees to arrive at results decisions for Travel Overtime and Compensatory Time In Lieu of Overtime travel. The static document (Travel Worksheets) has been automated to assist employees in deriving the appropriate conclusion as to whether or not time is compensable or not according the regulation and law.</p> <p>OATS – The OATS application is a desktop application that allows selected users to review, update, add and report tasks and assignments at various designated levels.</p> <p>MGCRB Case Tracker - The system is used to track cases/appeals received in the Office of Medicare Adjudication.</p> <p>MGCRB Calc - The system is used to track cases/appeals received in the Office of Medicare Adjudication.</p> <p>PRRB – The PRRB Case Tracker is used to track cases/appeals received in the Office of Medicare Adjudication. The system tracks actions taken on each case/appeal; tracks the participants associated with each case/appeal; tracks issues associated with each case/appeal; tracks hearing dates; and generates letters and reports as needed. The PRRB Case Tracker is written in Visual Basic and was developed for the Office of Hearings. The PRRB Case Tracker is a module of the Office of Hearings case tracking system. PRRB Case Tracker was implemented in 05/03. PRRB Case Tracker consists of a Microsoft Access database located on a shared drive in the CMS Data Center.</p> <p>COOP - The COOP system is used to manage the collection of contact information for individuals involved in the CMS Continuity of Operations Plan.</p> <p>OIGHTLNE – The OIG Hotline is used to store OIG Hotline complaints for Medicare Frauds &amp; Abuses purposes.</p> <p>ONREG – The CMS Online Registration System (ONREG) allows CMS employees to register for training courses and calendar events on-line via a web interface. The ONREG system is an integrated system that allows immediate access to training information, as well as, the ability to add and track training courses and calendar events.</p> <p>CMS Badge System – The CMS Badge system is an application that collects and houses necessary data to ensure that access to CMS Building, during both regular and security hours is restricted and to guard against unauthorized entry.</p>
13	Indicate if the system is new or an existing one being modified:	Existing
14	Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	Yes
15	Is the system subject to the Privacy Act?	Yes
16	If the system shares or discloses IIF please specify with whom and for what purpose(s):	No

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: Human Resources Management Systems

- 17

Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:
- Yes –All HRMS systems containing IIF information are subject to Rules of Behavior agreement and security protocols.  
CHRIS contains personally identifiable information of Name, SSN, DOB, Vehicle ID, Education, Employment Status, this information is used by Personnel and is only accessed by persons with management authority. The information is password protected with security protocols.  
ITSP-CBT - N/A  
FLSATRAV - N/A  
OATS - N/A  
PRRB - N/A  
OIGHTLNE - N/A  
COOP contains Name, SSN, Phone Numbers, Email Address and Work Location, this information is used by Personnel and is only accessed by persons with management authority. The information is password protected with security protocols.  
MGCRB contains Name, Mailing Address, Phone Numbers and Email Address, this information is used by Personnel and is only accessed by persons with management authority. The information is password protected with security protocols.  
ONREG contains Names and Email Addresses,  
CMS Badge contains Name, Work Location, Work Address and Phone Number and Photo Identification, this information is used by Personnel and is only accessed by persons with management authority. The information is password protected with security protocols.
- 18

Describe the consent process:
- The subject individual should write to the system manager who will require the system name, health insurance claim number, address, age, and sex and for verification purposes, the subject individual's name (woman's maiden name, if applicable) and social security number.
- 19

Does the system host a website?
- No
- 20

Does the website have any information or pages directed at children under the age of thirteen?
- No
- 21

Are there policies or guidelines in place with regard to the retention and destruction of IIF?
- Yes
- 22

Are there technical controls present?
- Yes
- 23

Describe the IIF security controls:
- CHRIS contains personally identifiable information of Name, SSN, DOB, Vehicle ID, Education, Employment Status, this information is used by Personnel and is only accessed by persons with management authority. The information is password protected with security protocols.  
ITSP-CBT - N/A  
FLSATRAV - N/A  
OATS - N/A  
PRRB - N/A  
OIGHTLNE - N/A  
COOP contains Name, SSN, Phone Numbers, Email Address and Work Location, this information is used by Personnel and is only accessed by persons with management authority. The information is password protected with security protocols.  
MGCRB contains Name, Mailing Address, Phone Numbers and Email Address, this information is used by Personnel and is only accessed by persons with management authority. The information is password protected with security protocols.  
ONREG contains Names and Email Addresses,  
CMS Badge contains Name, Work Location, Work Address and Phone Number and Photo Identification, this information is used by Personnel and is only accessed by persons with management authority. The information is password protected with security protocols.
- 24

Sr Official of Privacy Signature:
- Abby Block
- 25

Sr Official of Privacy Signoff Date:
- Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: IT Management Systems

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer "No" to that question.

2Summary of PIA Required Questions

Question	Response
1 System:	IT Management Systems
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-03-00-02-1010-00 009-38-02-00-01-1150-00
7 Privacy Act System of Records (SOR) Number:	09-70-3005
8 OMB Information Collection Approval Number:	N/A
9 Other Identifying Number(s):	N/A
10 System Name:	IT Management Services
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	Jerry J. Williams
12 Provide an overview of the system:	<p>The Correspondence Inquiry System (CIS) is the agency's correspondence tracking, receiving and document workflow system. It is used to collect and store internal and external document request, program inquiries, congressional inquiries, and the agency's responses to these inquiries and requests. It also allows the tracking and progress of work items and reassign them to different users, or components as necessary. It replaces hard-copy folders and documents with electronic files that can be routed easily to the next user or group involved with the document processing. It is currently a 16 bit application and can not be modified or upgraded with out significant cost.</p> <p>Existing</p>
13 Indicate if the system is new or an existing one being modified:	Existing
14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	Yes
15 Is the system subject to the Privacy Act?	Yes
16 If the system shares or discloses IIF please specify with whom and for what purpose(s):	System does not discloses or allow any information to be shared with other applications, agencies or outside sources.
17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:	System does not disclose or allow any information to be shared with other applications, agencies or outside sources. The agency does not actively collect the IIF information. It is often contained witin the request or correspondence (etc. letters, fax, documents) that may be used for correspondence with CMS
18 Describe the consent process:	No consent has been required, since any changes to the system will have no effect as to how the IIF data can be accessed. Storage of the information follows the privacy act guidelines and No information is shared or actively collected.
19 Does the system host a website?	No
20 Does the website have any information or pages directed at children under the age of thirteen?	No
21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?	Yes
22 Are there technical controls present?	Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

## CMS: IT Management Systems

- 23 Describe the IIF security controls:

The data is stored within an database as well as on a Document Storage Server. The only access granted is to current users of the application. The system has its own backup unit and the data is incrementally backed up each night and a full backup is scheduled for each weekend. Access to the servers is also on restrictive Access.  
As system administrator I view the data as falling under the Privacy ACT and have set the guidelines for the dissemination of data contained in the Correspondence Inquiry System.
- 24 Sr Official of Privacy Signature:

Abby Block
- 25 Sr Official of Privacy Signoff Date:

Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicaid & State Children's Health Insurance Systems

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer "No" to that question.

2

Summary of PIA Required Questions

Question

Response

- 1 System:

Medicaid & State Children's Health Insurance Systems
- 2 Is this a new PIA?

No
- 3 If this is an existing PIA, please provide a reason for revision:

PIA Validation
- 4 Date of this Submission:

Jun 29, 2007
- 5 OPDIV Name:

CMS
- 6 Unique Project Identifier (UPI) Number:

009-38-01-06-01-1010-00 009-38-01-04-01-1060-00
- 7 Privacy Act System of Records (SOR) Number:

09-70-0541
- 8 OMB Information Collection Approval Number:

CMS-416 OMB#0938-0354 Expiration Date: 03-31-2009;  
CMS-64 OMB# 0938-0067 Expiration Date: 06/30/2008,  
CMS-21 & 21B OMB# 0938-0731 Expiration Date 06/30/2008,  
CMS-37 OMB# 0938-0101 Expiration Date 06/30/2008;  
OMB# 0938-0707, Expiration Date 05/31/2008;  
OMB# 0938-0599, CMS-102 Expiration Date: 11/30/2007;  
OMB# 0938-0599, CMS-105 Expiration Date: 11/30/2007;OMB #  
0938-0345, Expiration Date: 07/31/2006;  
OMB# 0938-0707, Expiration Date: 05/31/2008
- 9 Other Identifying Number(s):

CMS-R-0284
- 10 System Name:

Medicaid & State Children's Health Insurance System
- 11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:

Dona Coffman; Cora Burch; Marcus Koenig

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicaid & State Children's Health Insurance Systems

- 12 Provide an overview of the system:
- EPSDT: The Early and Periodic Screening, Diagnostic and Treatment (EPSDT) Data System is a web-based Intranet application for use by the Centers for Medicare & Medicaid Services (CMS).
- The annual EPSDT Report (Form CMS-416) provides basic information on participation in the Medicaid child health program. The information is used to assess the effectiveness of State EPSDT programs in terms of the number of children (by age group and basis of Medicaid eligibility), who are provided child health screening services, referred for corrective treatment, and the number receiving dental services. Child health-screening services are defined, for purposes of reporting on Form CMS-416, as initial periodic screens required to be provided according to a State's screening periodicity schedule.
- The complete report demonstrates the State's attainment of its participant and screening goals. Participant and screening goals are two different standards against which EPSDT participation is measured on the Form CMS-416. From the completed reports, trend patterns and projections are developed for the nation and for individual States or geographic areas, from which decisions and recommendations can be made to ensure that eligible children are given the best possible health care. This information is also used to respond to congressional and public inquiries.
- FULs: The Federal Upper Limit System (FULs) determines the highest allowable Medicaid price for Federal Drug Administration (FDA) approved drugs. This price is derived from manufacturer prices obtained from external sources: Medispan, Blue Book and Red Book. The primary output from this system is the "Payment for Services Report" which lists all products along with their strengths, dosage form, route of administration, package size, the FULs price and source.
- SPW: The State Plan Amendment and Waiver Tracking System (SPW) is an information tracking system that tracks State Plan Amendments and Waivers from their initial submittal to their final determination in a common format and Central Office database. This system tracks the following: State Plan Amendments (SPA), PACE SPAs, SCHIP SPAs, 1115 waivers, 1115 Independence Plus waivers, 1915(b) waivers, 1915(c) waivers, and 1915(c) Independence Plus waivers.
- MDR: The Medicaid Drug Rebate (MDR) System is composed of an online and batch system that collects drug manufacturers product and price information and state drug utilization data for drugs given to State Medicaid recipients. The system calculates the quarterly unit drug rebates that are then sent to the states for invoicing drug manufacturers each quarter.
- MBES/CBES: MBES\CBES collects and stores States Medicaid budgets & expenditure information. The system is used by states to submit budget and expenditure data for the Medicaid and State Children's Health Insurance Program to CMS. CMS' Regional Office personnel review the state submissions and enter analysis into the system. All activity is reviewed and certified by CMS Central Office personnel. Summarized data from this information is publicly available on the CMS Public web site.
- SCHIP/SEDS: The State Children's Health Insurance Program (SCHIP) Statistical Database Enrollment System (SEDS) is a system that states use to submit enrollment and demographic data for the SCHIP Program to CMS. CMS' Regional Office personnel review the state submissions and enter analysis into SCHIP SEDS. All of this activity is reviewed and certified by CMS Central Office personnel.

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicaid & State Children's Health Insurance Systems

	IBNRS: The Incurred But Not Reported Survey system is a web-based application used by CMS biannually both to report estimated expenditures for the Medicaid Programs and State Children's Health Insurance Program. The purpose of the IBNRS application is to create an online version of two forms - the CMS-R199, Form for the Medicaid Accounts Payable and Accounts Receivable as well as the CMS-10180, Form for the SCHIP Accounts Payable and Acc Existing
13 Indicate if the system is new or an existing one being modified:	
14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	Yes
15 Is the system subject to the Privacy Act?	Yes
16 If the system shares or discloses IIF please specify with whom and for what purpose(s):	EPSDT: N/A FULs: N/A SPW: N/A MDR: N/A MBES/CBES: N/A SCHIP SEDS: N/A IBNRS: N/A S&C/CLIA: N/A MSIS/MAX: Census Bureau for state population, Congressional Budget Office and for analysis and research purposes and organizations operating under an approved Data User Agreement such as the Urban Institute. TIPS: N/A SARTS: N/A DDR: N/A
17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:	EPSDT: N/A FULs: N/A SPW: N/A MDR: N/A MBES/CBES: N/A SCHIP/SEDS: N/A IBNRS: N/A S&C/CLIA: N/A MSIS/MAX: Date of Birth, Social Security Number TIPS: N/A SARTS: N/A DDR: N/A
18 Describe the consent process:	EPSDT: N/A FULs: N/A SPW: N/A MDR: N/A MBES/CBES: N/A SCHIP SEDS: N/A IBNRS: N/A S&C/CLIA: N/A MSIS/MAX: HIPAA Disclosure policy TIPS: N/A SARTS: N/A DDR: N/A
19 Does the system host a website?	Yes
20 Does the website have any information or pages directed at children under the age of thirteen?	No
21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?	Yes
22 Are there technical controls present?	Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicaid & State Children's Health Insurance Systems

- 23 Describe the IIF security controls:
- EPSDT: Rules of Least Privilege; Authorized personell with approved user ID and password; firewall and intrusion detection; Guards; Identification Badges; Key Cards
- FULs: Rules of Least Privilege; Authorized personell with approved user ID and password; firewall and intrusion detection; Guards; Identification Badges; Key Cards
- SPW: Rules of Least Privilege; Authorized personell with approved user ID and password; firewall and intrusion detection; Guards; Identification Badges; Key Cards
- MDR: Rules of Least Privilege; Authorized personell with approved user ID and password; firewall and intrusion detection; Guards; Identification Badges; Key Cards
- MBES/CBES: Rules of least privilege; authorized personnel with approved user Id and password; firewall and intrusion detection; Identification Badges; Key Cards; Closed Circuit TV (CCTV)
- SCHIP/SEDS: Rules of least privilege; authorized personnel with approved user Id and password; firewall and intrusion detection; Identification Badges; Key Cards; Closed Circuit TV (CCTV)
- IBNRS: Rules of least Privilege; authorized personnel with approved user ID and password; firewall and intrusion detection; Identification Badges; Key Cards; Close Circuit TV
- S&C/CLIA: Rules of least privilege; authorized personnel with approved user Id and password; firewall and intrusion detection; Identification Badges; Key Cards; Closed Circuit TV (CCTV)
- MSIS/MAX: Rules of Least Privilege; Authorized personell with approved user ID and password; firewall and intrusion detection; Guards; Identification Badges; Key Cards
- TIPS: Rules of Least Privilege; Authorized personell with approved user Id and password; firewall and intrusion detection; Guards; Identification Badges; Key Cards;
- SARTS: Rules of least privilege; authorized personnel with approved user Id and password; firewall and intrusion detection; Identification Badges; Key Cards; Closed Circuit TV (CCTV)
- DDR: Rules of least Privilege; authorized personnel with approved user ID and password; firewall and intrusion detection; Identification Badges, Key Cards, Closed Circuit TV
- 24 Sr Official of Privacy Signature: Abby Block
- 25 Sr Official of Privacy Signoff Date: Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicare Advantage and Prescription Drug Plan Operation System

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

2

## Summary of PIA Required Questions

### Question

### Response

- 1

System:
- Medicare Advantage and Prescription Drug Plan Operation System
- 2

Is this a new PIA?
- No
- 3

If this is an existing PIA, please provide a reason for revision:
- PIA Validation
- 4

Date of this Submission:
- Jun 29, 2007
- 5

OPDIV Name:
- CMS
- 6

Unique Project Identifier (UPI) Number:
- 009-38-01-04-01-1090-00 009-38-01-04-02-1080-00  
009-38-01-04-02-1095-00 009-38-01-04-01-1085-00  
009-38-01-04-01-1075-00 009-38-02-00-01-1150-00  
09-70-4001, 09-70-4004, 09-70-0552, 09-70-0553
- 7

Privacy Act System of Records (SOR) Number:
- N/A
- 8

OMB Information Collection Approval Number:
- N/A
- 9

Other Identifying Number(s):
- N/A
- 10

System Name:
- Medicare Advantage and Prescription Drug Plan Operation System
- 11

System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:
- Marni Land, 410-786-2258

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

- 12 Provide an overview of the system:
- APPS - PROCESS AND MAINTAIN PAYMENT INFORMATION FOR MEDICARE ADVANTAGE PLAN AND PRESCRIPTION DRUG PLANS.
- DDPS – The DDPS is being developed to support CMS’ implementation of the new Medicare Prescription Drug Benefit program, mandated by the Medicare Prescription Drug, Improvement and Modernization Act (MMA) of 2003. This system will process all Medicare covered and non-covered drug events, including non-Medicare drug events, for Medicare beneficiaries participating in the Part D programs. The system will process Prescription Drug Event (PDE) transactions and related data as necessary to validate/authenticate Medicare payment of covered drugs made by plans for enrolled Medicare beneficiaries
- HPMS – HPMS is a web-enabled Extranet information system that supports numerous business functions of the Medicare Advantage and Part D programs, including plan application submission and review, formulary submission and review, bid submission and review, complaints tracking, and plan oversight.
- MARX – MARx is an enhancement of the Medicare Managed Care System (MMCS), with changes for the implementation of the Medicare Modernization Act (MMA).
- MIIR – MIIR is a data repository created to report on Medicare Beneficiary Part D information at the aggregate level in support of MMA. Currently, MIIR has counts to be used for analysis on aspects of beneficiaries such as demographics, LIS, enrollment information, etc via a reporting tool. This system is used by CMS internal staff only.
- PWS – The Premium Withhold Subsystem tracks Part C and/or Part D beneficiary level premium payments for the entire Medicare population (approximately 40 million beneficiaries) who elect either Part C - Medicare Advantage - or Part D - Medicare prescription drug coverage, including managing the data exchange for Medicare beneficiaries who elect to have their premiums withheld by OPM, SSA, or RRB.
- RAS – The Risk Adjustment Suite of Software are modules within the Medicare Modernization Act (MMA) program. The Risk Adjustment Suite of Software receives diagnostic and beneficiary data from other systems, stages the data, calculates Risk Adjustment Factors (RAFTs), feeds the RAFTs to other systems within MMA, and provides reports on the resulting factors.
- TROOP - This system provides MBD and COB info to the TrOOP facilitator.
- SPDBS- The SPDBS is the CMS system of record for billing and processing the collection on monies from the states to defray a portion of the Medicare drug expenditures for individuals whose projected Medicaid drug coverage is assumed by Medicare Part D. The SPDBS was developed as a COBOL program and flat file batch process and resides on the mainframe at the CMS Computer Center. The SPDBS does not interface with any databases of CICS.
- MPC: Determines the Medicare Plus Choice payment rates for every State by county. These rates are fed into the Automated Plan Payment System Database. The APPS uses these rates to make payments on behalf of MEDicare beneficiaries who choose to obtain Medicare benefits through private health plans under the MEDicare Advantage program.
- AAPCC: Supports payment to Medicare Advantage plans by feeding

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicare Advantage and Prescription Drug Plan Operation System

- 13 Indicate if the system is new or an existing one being modified:
- 14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?
- 15 Is the system subject to the Privacy Act?
- 16 If the system shares or discloses IIF please specify with whom and for what purpose(s):

essectial information and data into the MEdicare Advantage System. The AAPCC application captures Medicare enrollment and demographic data that is used as input to the Medicare Advantage application which calculated payment rates to managed care organizations. A by-product of this system is the tabulation of annual Medicare reimbursement and enrollment on a county basis. The enrollment includes all MEdicare beneficiaries, whereas the reimbursement includes only claims paid by intermediaries and carriers, i.e., it excludes capitation payments made to HMO and similar organizations.

Existing

Yes

Yes  
APPS – OFM FACS system

DDPS – All reporting/data access is restricted to mandated and authorized users of the data with statutory authority as described in the MMA legislation, which includes:  
Those necessary to implement, operate, and support the developed system;  
The CSSC at Palmetto requiring PDE and beneficiary data access;  
The MDBG within CBC responsible for benefit implementation, program administration, and program oversight;  
The Medicare PIG within OFM responsible for protecting program integrity and detecting waste, fraud, and abuse of the program;  
The QIO contracted by OCSQ responsible for clinical quality and evaluation of health care outcome of the benefit; and  
The 723 initiative being coordinated by ORD1 responsible for developing integrated databases.

HPMS – HPMS will make the complaints tracking data available via reports and extracts to CMS staff for plan oversight and monitoring. It may also be necessary to share these data with other federal agencies (e.g., FBI, OIG) if further investigation of a Part D organization is required.

MARX – Internal – MBD for determining beneficiary demographic data and identifying information, RAS for risk adjustment rates, PWS for withholding data Gentran / EFT for communicating beneficiary and plan data, NGD for processing disenrollments from the 1800Medicare, Retiree Drug Subsidy (RDS) for rejected enrollments, and IACS for identity management of users.

MIIR – No

PWS – External – SSA, to be able to provide withholding information for beneficiaries  
Internal – MARx, MBD to get information about beneficiaries and plans.

RAS – Internal – MARx, MBD for determining beneficiary demographic data and identifying information, NMUD for diagnosis data of a beneficiary

TROOP – N/A  
SPDBS: N/A.  
MPC: N/A.  
AAPCC: N/A

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:

APPS – PART C AND PART D PAYMENT DOLLARS.

DDPS – The system contains both detailed and summary prescription drug claim information on all Medicare covered and non-covered drug events, including non-Medicare drug events, for Medicare beneficiaries of the Medicare program. This system contains both detailed and summary prescription drug claim data, health insurance claim number, card holder identification number, date of service, gender, and optionally, the date of birth. The system contains provider characteristics, prescriber identification number, assigned provider number (facility, referring/servicing physician), and national drug code. The system contains beneficiary, plan, and supplemental payment amounts. Submission of IIF is mandatory - as a condition of payment, all Part D plans must submit data and information necessary for CMS to carry out payment provisions.

HPMS – HPMS collects the name, mailing address, e-mail address, and/or phone number of the beneficiary reporting a complaint related to the Part D program. All fields are optional. CMS will use these data to resolve beneficiary complaints and track plan performance.

MARX – MARX is not the system of record (SOR) for IIF , but it does store and process IIF regarding system users, beneficiary’s healthplan enrollment and plan payment information. The enrollment of beneficiaries into healthplans is provided from the plans, or from the deeming and autoenrollment enrollments from MBD. Policies regarding the voluntary or mandatory nature of the IIF are the responsibility of the systems that provide the enrollment transactions to MARx.

MIIR – MIIR maintains Beneficiary demographics, LIS, and enrollment information from other CMS source systems to be used for reporting aggregate numbers by CMS staff in support of Executive management needs for MMA Part D reporting and analysis.

PWS – PWS is not the system of record (SOR) for IIF , but it does store and process IIF regarding beneficiary’s healthplan enrollment, plan payment information., and individual’s social security status and identifiers. Policies regarding the voluntary or mandatory nature of the IIF are the responsibility of the systems that provide the beneficiaries or plan data to PWS.

RAS – RAS assesses the health risk presented by Beneficiaries to enable the MMCS to produce an appropriate risk based payment to the Managed Care Organizations (MCO). Additionally, RAS requires information from several other application systems. RAS is not the system of record (SOR) for ANY of the IIF, but it does store and process IIF. Policies regarding the voluntary or mandatory nature of the IIF are the responsibility of the SORs for that IIF.

TROOP – Disseminate eligibility/ enrollment and 4Rx data to pharmacists and COB info to plans.

SPDBS: Once a month, the SPDBS receives as input three flat files provided by CMS internal components. CMSO and the MBD provide one dataset containing a count of the number of new Medicare beneficiary enrollments and disenrollments for which the states are to be held responsible. OACT provides on dataset containing the monthly state billing rates to be applied. OFM provides on dataset containing a record of the state payments that have been posted in the previous month. SPDBS simply receives the new state enrollment counts from the MBD, multiplies those numbers by the billing rates from OACT to generate a new state liability charge. SPDBS then develops a Summary Accounting Statement showing the previous months balance, the payments posted provided by OFM, the new liability charges that have been calculated, and the resulting new

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Medicare Advantage and Prescription Drug Plan Operation System

account balance. All this information is also recorded in a state account ledger and other CMS billing summary documentation.

AAPCC: Supports payment to MEdicare Advantage plans by feeding essential information and data into the Medicare Advantage System. The AAPCC application captures Medicare enrollment and demographic d

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Medicare Advantage and Prescription Drug Plan Operation System

18	Describe the consent process:	<p>APPS – NONE</p> <p>DDPS – Participation in Part D is voluntary and requires an affirmative election to join. When an individual enrolls in a Part D Plan, as part of the application package, the beneficiary has to sign the Agreement page; thus, MMA Part D enrollment equates beneficiary consent.</p> <p>Authority for maintenance of this system is given under provisions of the Medicare Prescription Drug, Improvement, and Modernization Act, amending the Social Security Act (the Act) by adding Part D under Title XVIII (§ 1860D–15(c)(1)(C) and (d)(2), as described in 42 Code of Federal Regulation (CFR) 423.401.</p> <p>The Privacy Act permits us to disclose information without an individual’s consent if the information is to be used for a purpose that is compatible with the purpose(s) for which the information was collected. Any such disclosure of data is known as a “routine use.”</p> <p>This system contains Protected Health Information as defined by HHS regulation “Standards for Privacy of Individually Identifiable Health Information” (45 CFR Parts 160 and 164, 65 FR 82462 (Dec. 28, 00), as amended by 66 FR 12434 (Feb. 26, 01)). Disclosures of Protected Health Information authorized by these routine uses may only be made if, and as, permitted or required by the “Standards for Privacy of Individually identifiable Health Information.”</p> <p>In addition, our policy will be to prohibit release even of non-identifiable information, except pursuant to one of the routine uses, if there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the patient population is so small that individuals who are familiar with the enrollees could, because of the small size, use this information to deduce the identity of the beneficiary).</p> <p>In addition, CMS will make disclosure from the proposed system only with consent of the subject individual, or his/her legal representative, or in accordance with an applicable exception provision of the Privacy Act.</p> <p>CMS, therefore, does not anticipate an unfavorable effect on individual privacy as a result of the disclosure of information relating to individuals.</p> <p>HPMS – There is no process in-place at this time.</p> <p>MARX – MARx is fed IIF from MBD, and healthplan systems, and passes information to MBD and healthplans. MARx is not the SOR for the IIF, so there are no agreements in place from MARx with the individuals regarding IIF.</p> <p>MIIR – NO</p> <p>PWS – PWS is fed IIF from MBD and MARx internal CMS systems, and data from external SSA and RRB systems via CMS Enterprise Data Exchange. PWS is not the SOR for the IIF.</p> <p>RAS – RAS is fed IIF from MBD, and RAS internal CMS systems, and passes information to MARx. RAS is not the SOR for the IIF</p> <p>TROOP – NO</p> <p>SPDBS - N/A</p>
----	-------------------------------	---

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicare Advantage and Prescription Drug Plan Operation System

AAPCC: N/A

MPC: N/A

Yes

No

Yes

Yes

- 19 Does the system host a website?
- 20 Does the website have any information or pages directed at children under the age of thirteen?
- 21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?
- 22 Are there technical controls present?

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

23	Describe the IIF security controls:	<p>APPS – RACF controls are in place per the GSS and EUA systems as far as technical and administrative electronic access to records, and the data center controls physical access.</p> <p>DDPS – CMS has safeguards in place for authorized users and monitors such users against excessive or unauthorized use. Personnel having access to the system have been trained in the Privacy Act and information security requirements. Employees who maintain records in this system are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access. This system will conform to all applicable Federal laws and regulations and Federal, HHS, and CMS policies and standards as they relate to information security and data privacy. These laws and regulations include but are not limited to: the Privacy Act of 1974; the Federal Information Security Management Act of 2002; the Computer Fraud and Abuse Act of 1986; the Health Insurance Portability and Accountability Act of 1996; The EGovernment Act of 2002, the Clinger-Cohen Act of 1996; the Medicare Modernization Act of 2003, and the corresponding implementing regulations. OMB Circular A-130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources also applies. Federal, HHS, and CMS policies and standards include but are not limited to: all pertinent National Institute of Standards and Technology publications; the HHS Information Systems Program Handbook and the CMS Information Security Handbook.</p> <p>HPMS – HPMS utilizes the following control mechanisms: user ID and password-controlled access, firewall, Virtual Private Network technology, encryption, and intrusion detection (technical controls); guards, identification requirements, key cards (physical controls at hosting facility); systems security plan, contingency plan, regular backups, and personnel training (administrative controls).</p> <p>MARX – RACF controls are in place per the GSS and EUA systems as far as technical and administrative electronic access to records, and the data center controls physical access.</p> <p>MIIR – Users of MIIR do not have beneficiary level (IIF) access. Prior to access to aggregate data being granted, a business owner listed within EUA receives a request from a user. The user must first have MIIR Training, submit a DUA, and provide a business reason for requiring the access. If all of that is satisfactory, the business owner approves the request for access to the aggregate level information. This process is handled through CMS’s CAA, EUA, and LDAP processes so that all agency related policies for access request, approval, and password protection are utilized.</p> <p>PWS – RACF controls are in place per the GSS and EUA systems as far as technical and administrative electronic access to records, and the data center controls physical access.</p> <p>RAS – RACF controls are in place per the GSS and EUA systems as far as technical and administrative electronic access to records, and the data center controls physical access.</p> <p>TROOP – Contractor must follow the CMS “System Security Plan and Risk Assessment Guidelines” which is based on the NIST special publication “Guide for Developing Security Plans for Information Technology Systems”</p> <p>AAPCC: N/A MPC: N/A SPDBS: N/A</p>
----	-------------------------------------	--

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicare Advantage and Prescription Drug Plan Operation System

24 Sr Official of Privacy Signature: Abby Block

25 Sr Official of Privacy Signoff Date: Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicare Appeals Systems

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer "No" to that question.

2

Summary of PIA Required Questions

Question	Response
1 System:	Medicare Appeals Systems
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-01-04-01-1180-00
7 Privacy Act System of Records (SOR) Number:	09-70-0566
8 OMB Information Collection Approval Number:	N/A
9 Other Identifying Number(s):	N/A
10 System Name:	Medicare Appeals System
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	Aaron Pleines
12 Provide an overview of the system:	The Medicare Appeals System allows both tracking of and reporting on the Medicare appeals process. This system is used to support the new Medicare process established by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) and the Benefits Improvement and Protection Act of 2000 (BIPA).
13 Indicate if the system is new or an existing one being modified:	Existing
14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	Yes
15 Is the system subject to the Privacy Act?	Yes
16 If the system shares or discloses IIF please specify with whom and for what purpose(s):	The Office of Medicare Hearings and Appeals (OMHA), CMS, and the CMS contractors who process Medicare appeals. The IIF is necessary to record and adjudicate the Medicare appeals. The MAS will collect and maintain IIF in order to record and adjudicate appeals of Medicare claims and services in dispute. This information may include: Name, Health Insurance Claim Number (HICN), Social Security Number, Address, Telephone Number, Medical History, and other personal information necessary to conduct a review of the appeal. The Medicare Appeals System will collect and maintain beneficiary enrollment data, claim information, and contact information. This information will include Information in Identifiable Form (IIF) that will be held to the highest confidentiality. Submission of this information is mandatory for anyone requesting an appeal on their claim.
17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:	The MAS System of Record provides notification of the data that will be collected and maintained. Written notice is provided in the MAS system of records.
18 Describe the consent process:	Yes
19 Does the system host a website?	No
20 Does the website have any information or pages directed at children under the age of thirteen?	Yes
21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?	Yes
22 Are there technical controls present?	Yes
23 Describe the IIF security controls:	Users are required to wear Identification Badges / Key Cards in order to gain access to the facilities. The user must then access the system through a T1 line that is dedicated to CMS. Firewalls are in place to block unauthorized access. The user can only access the system with their CMS userid and password. This password expires after 60 days, has a minimum length of eight characters, and accounts are locked after three incorrect attempts. Accounts are also logged out after 15 minutes of inactivity. User accounts are also role based to protect unnecessary access to IIF.
24 Sr Official of Privacy Signature:	Abby Block

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicare Appeals Systems

25 Sr Official of Privacy Signoff Date: Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicare Beneficiary Enrollment Systems

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

2

Summary of PIA Required Questions

Question	Response
1 System:	Medicare Beneficiary Enrollment Systems
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-01-09-01-1120-00 009-38-01-04-01-1150-00
7 Privacy Act System of Records (SOR) Number:	09-70-0502, 09-70-0536
8 OMB Information Collection Approval Number:	N/A
9 Other Identifying Number(s):	N/A
10 System Name:	Medicare Beneficiary Enrollment Systems
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	EDB/MBD: Anthony Culotta, Director Medicare appeals and Enrollment Group; Karen Fedi, Division Director, Division of Premium Billing & Collections
12 Provide an overview of the system:	<p>The EDB is a collection of automated systems that support the collection and maintenance of information (e.g., demographics, enrollment, insurance, premium payments) about Medicare beneficiaries.</p> <p>The MBD was developed to provide CMS with a centralized database that supports the collection and maintenance of information about Medicare Program beneficiaries. The Medicare beneficiary information contained in the MBD is used to support managed care enrollments, payments to Managed Care Organizations, and the Prescription Drug Program. Specifically for DBS, to produce appropriate and accurate bills for and track the collection of Medicare Hospital Insurance (HI) premiums (Part A) and Supplementary Medical Insurance (SMI) premiums (Part B). Specifically for TPS, to perform third party premium billing and collection operations.</p> <p>Existing</p>
13 Indicate if the system is new or an existing one being modified:	Existing
14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	Yes
15 Is the system subject to the Privacy Act?	Yes
16 If the system shares or discloses IIF please specify with whom and for what purpose(s):	Public citizens, business partners/contacts (Federal, State, local agencies), etc., as stated under the Routine Uses outlined in the System of Records for the MBD and EDB.
17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:	<p>The agency collects information related to Medicare enrollment and entitlement and Medicare Secondary Payer data containing other party liability insurance information necessary for appropriate Medicare claim payment. It contains hospice election, premium billing and collection, direct billing information, and group health plan enrollment data. It also contains the individual’s health insurance numbers, name, geographic location, race/ethnicity, sex, and date of birth. Information is collected on individuals age 65 or over who have been, or currently are, entitled to health insurance benefits under Title XVIII of the Act or under provisions of the Railroad Retirement (RR)Act, individuals under age 65 who have been or currently are, entitled to such benefits on the basis of having been entitled for not less than 24 months to disability benefits under Title II of the Act or under the RR Act, individuals who have been, or currently are, entitled to such benefits because they have ESRD, individuals age 64 and 8 months or over who are likely to become entitled to health insurance benefits upon attaining age 65, and individuals under age 65 who have at least 21 months of disability benefits who are likely to become entitled to Medicare upon the 25th month of their being disabled. It is a voluntary collection.</p>

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Medicare Beneficiary Enrollment Systems

- 18 Describe the consent process:

The information is collected from Medicare beneficiaries and obtained by CMS. The beneficiaries are informed that CMS will only disclose the minimum personal data necessary to achieve the purpose of the Enrollment Database and under what routine uses the information will be disclosed. By law, CMS is required to protect the privacy of individual's personal medical information. CMS is also required to give individuals notice telling them how CMS may use and disclose their personal medical information. Individuals are made aware in the 'Medicare and You Handbook' published yearly and sent out to each Medicare beneficiary. Individuals have the right to amend any medical information that they believe to be incorrect, get a listing of anyone the information is disclosed to, and ask CMS to limit how their personal medical information is used and given out to pay claims and run the Medicare program.  
All notice of consent will be given in written form.
- 19 Does the system host a website?

No
- 20 Does the website have any information or pages directed at children under the age of thirteen?

No
- 21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?

Yes
- 22 Are there technical controls present?

Yes
- 23 Describe the IIF security controls:

The system was certified and accredited to process MBES data 02/2007. A draft of the System Security Plan (SSP) and Risk Assessment (RA) was completed for review 06/06 and 05/06 respectively. SSP Security controls are routinely reviewed, a contingency plan is in place and files are backed up and stored offsite regularly. All personnel (users, administrators, developers, contractors) using the system have been trained and made aware of their responsibility to protect the data collected and maintained.

Technical controls (user ids, passwords, firewalls) are in place to minimize the possibility of unauthorized access, use or dissemination of the data in the system.

Unauthorized access messages are generated by the system and forwarded to the appropriate CMS personnel for investigation. Physical access controls (guards, identification badges, key cards, closed-circuit TV) are also in place.
- 24 Sr Official of Privacy Signature:

Abby Block
- 25 Sr Official of Privacy Signoff Date:

Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicare Claims Processing Systems

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer "No" to that question.

2

Summary of PIA Required Questions

Question	Response
1 System:	Medicare Claims Processing Systems
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-01-06-01-1110-00 009-38-01-06-01-1120-00 009-38-01-06-01-1130-00 009-38-01-06-01-1140-00 009-38-01-06-02-1150-00 009-38-01-04-01-1160-00 09-70-0526, 09-70-0558, 09-70-0505, 09-70-0537, 09-70-0572
7 Privacy Act System of Records (SOR) Number:	n/a
8 OMB Information Collection Approval Number:	n/a
9 Other Identifying Number(s):	n/a
10 System Name:	Medicare Claims Processing Systems
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	Karen Jackson
12 Provide an overview of the system:	The Medicare Claims Processing System is a collection of systems hosted in Medicare contractors' data centers to process Medicare claims for reimbursement. Existing
13 Indicate if the system is new or an existing one being modified:	Existing
14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	Yes
15 Is the system subject to the Privacy Act?	Yes
16 If the system shares or discloses IIF please specify with whom and for what purpose(s):	IIF is shared with patients, business partner/contacts, and vendors/supplier/contractors to verify receipt of service and properly pay claims. The information collected, maintained or disseminated includes name, date of birth, social security number, mailing address, phone numbers, medical record numbers, medical notes, financial account information and/or numbers, certificates, device identifiers, email address, military status and/or records, employment status and/or records, employer or school name, health insurer name/plan, health insurer group number, patient marriage and employment status, CMS-1450 (UB92), CMS-1500 (ANSI X12 837) for the purpose of processing and paying claims. The information contains IIF. The submission of the personal information is mandatory.
17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:	System of records and the Medicare & You handbook. The handbook is used to annually notify individuals of their right to ask Medicare to limit how their IIF is used and given out to pay their claims and run the Medicare program.
18 Describe the consent process:	
19 Does the system host a website?	No
20 Does the website have any information or pages directed at children under the age of thirteen?	No
21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?	Yes
22 Are there technical controls present?	Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Medicare Claims Processing Systems

- 23 Describe the IIF security controls:

Access to the systems is given based on need to know and job responsibilities to process Medicare claims. Medicare Claims Processing Standard Systems maintainers use security software and methods to provide “least privilege access.” They will utilize packages such as RACF or ACF2 to grant or deny access to data based upon need to know. Sometimes, in order to fix programmatic problems, programmers are granted temporary access in order to fix and ensure that errors are fixed. The temporary access may be granted for a day or other short periods of time that can be controlled through security software. External audits also verify these controls. Technical controls used include user identification, passwords, firewalls, virtual private networks and intrusion detection systems. Physical controls used include guards, identification badges, key cards, cipher locks and closed circuit televisions.
- 24 Sr Official of Privacy Signature:

Abby Block
- 25 Sr Official of Privacy Signoff Date:

Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicare Data Centers

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

2 Summary of PIA Required Questions

Question	Response
1 System:	Medicare Data Centers
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-01-04-01-1030-00
7 Privacy Act System of Records (SOR) Number:	N/A
8 OMB Information Collection Approval Number:	N/A
9 Other Identifying Number(s):	N/A
10 System Name:	Medicare Data Centers
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	Charlene Fletcher

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicare Data Centers

- 12 Provide an overview of the system:

Congress established the Medicare Program in 1965 when it enacted Title XVIII of the Social Security Act. The Medicare Program is a Federal health insurance program and now serves over 40 million beneficiaries and processes over 900 million claims per year. To ensure a quick and smooth implementation of the Medicare program in 1965, Congress adopted an administrative structure, which was compatible with the historical pattern of administration used by the private health insurance industry. This allowed the Federal Government to contract with existing public or private organizations to facilitate services to beneficiaries and providers of health care services. It also allowed many systems to be developed for Medicare claims processing.

Traditional Fee-For-Service (FFS) coverage in the Medicare Program consists of two distinct parts. Hospital insurance (Part A of the Program) covers expenses for medical services furnished in institutional settings, such as hospitals or skilled nursing facilities, or services provided by a home health agency or hospice. Supplemental medical insurance (Part B of the Program) covers physician and other practitioner services; certain durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS) services; and other outpatient services.

Medicare FFS Claims are processed by Fiscal Intermediaries (FIs), Carriers, and Durable Medical Equipment Regional Carriers (DMERCs) using the family of shared systems described below:

**Part A Shared System**  
Hospital insurance claims process through the Fiscal Intermediaries Shared System (FISS), which performs claims processing and benefit payment functions for institutional providers under Parts A and B of the program. The Medicare contractors that use FISS are known as “fiscal intermediaries” (FIs).

**Part B Shared System**  
The Part B Shared System supports the processing of Medicare Part B claims. Medicare Part B is supplemental medical insurance, which covers physician services and other outpatient services. The Shared System for Part B Medicare is the Multi Carrier System (MCS). Medicare Part B claims processing contractors are known as Carriers, and include the Railroad Retirement Board. They process physician and supplier claims provided under Medicare Part B coverage.

**Durable Medical Equipment Regional Contractor (DMERC) Shared System**  
CMS has designated four carriers to have exclusive responsibility for handling Medicare Part B claims for Durable Medicare Equipment Prosthetics, Orthotics, and Supplies (DMEPOS) claims in specified geographic regions of the United States. They are commonly referred to as the “Durable Medical Equipment Regional Carriers (DMERCs).” The selected DMERCs currently use the VMS DME Shared system to process DMEPOS claims.
- 13 Indicate if the system is new or an existing one being modified:

Existing
- 14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?

Yes
- 15 Is the system subject to the Privacy Act?

No

**Note on IIF:** Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. **Note:** If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. **Note:** If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Medicare Data Centers

- 16

If the system shares or discloses IIF please specify with whom and for what purpose(s):
- The agency may share the collected information with a variety of Federal, state, local, and tribal government audiences and professional audiences, including the medical community. This includes, Providers, Ambulance Services, Medigap Companies / Supplemental Insurers, Clinical Labs, CMS contractors, DME Suppliers, Health Plans, Hospitals, Home Health Agencies, Physicians, Potential Contractors, Researchers, Skilled Nursing Facilities, and Suppliers.

Describe information collected

Please see hyperlinks to CMS forms below.
- 17

Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:
- Use of information collected

This information is used to process claims and payments for the Medicare Program beneficiaries. Submission of this information is mandatory and includes IIF.

Collection requirements

The Agency, through Medicare contractors and beneficiaries collects information through CMS forms CMS-1450 and CMS-1500. These are OMB approved forms.

Information is collected primarily through electronic means.

Form CMS-1450 (UB-92):

The UB-92 form and instructions are used by institutional and other selected providers to complete a Medicare Part A paper claim for submission to Medicare Fiscal Intermediaries. The paper UB-92 (Form CMS-1450) is neither a government printed form nor distributed by the CMS. The National Uniform Billing Committee (NUBC) is responsible for the design of the form (<http://www.nubc.org/>).

Form CMS-1500: Non-institutional providers and suppliers use CMS-1500 form and instructions to bill Medicare Part B covered services. It is also used for billing some Medicaid covered services. CMS -1500 (Health Insurance Claims Form) answers the needs of many health insurers. It is the basic form prescribed by CMS for the Medicare and Medicaid programs for claims submitted by physicians and suppliers, except for ambulance services. It has also been adopted by CHAMPUS and has the approval of the AMA Council on Medical Services. See link below for an electronic copy of form 1500.

Electronic Data Interchange (EDI) Enrollment Form

An organization comprising of multiple components that have been assigned Medicare provider numbers, supplier numbers, or UPINs may elect to execute a single EDI Enrollment Form on behalf of the organizational components to which these numbers have been assigned. The organization as a whole is to be held responsible for the performance of its components. The CMS Standard EDI Enrollment Form must be completed prior to submitting electronic media claims (EMC) to Medicare. Each provider of health care services, physician, or supplier that intends to submit EMC must execute the agreement. Each new EMC biller must sign the form and submit it to their local Medicare carrier or fiscal intermediary. Any existing EMC billers who have not completed the CMS Standard EDI Enrollment Form must complete and sign this form and submit it to their local Medicare carrier or fiscal intermediary also.

Please see the CMS Web page link listed below for information on:

Form CMS-1450 (UB92)

Form CMS-1500

Medicare Part A EDI Helpline

Medicare Part B EDI Helpline

EDI Enrollment Form and Instructions

<http://www.cms.hhs.gov/electronicbillingeditrans/>

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Medicare Data Centers

- 18 Describe the consent process:

Information is collected from two CMS forms, the 1450 and 1500. All Medicare Claims Processing Contractors are called 'satellites' under CWF. Satellites access the Host CWF databases to obtain needed beneficiary information. Satellites submit claims to the CWF Host for prepayment review and approval. Medicare beneficiaries are provided healthcare services where their personal information is collected and required for payment and reimbursement purposes. Beneficiaries receive HIPAA disclosure information by providers and Medicare directly. A complaint process is in place for individuals to raise their privacy concerns.
- 19 Does the system host a website?

No
- 20 Does the website have any information or pages directed at children under the age of thirteen?

No
- 21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?

Yes
- 22 Are there technical controls present?

Yes
- 23 Describe the IIF security controls:

The Medicare Claims Processing Systems incorporate a variety of security measures to protect IIF. These security measures include physical (e.g. use of access card readers, locked doors, cipher locks, and guards to control, restrict and monitor access), administrative (e.g. annual training of staff on security awareness and roles and responsibilities as well as background checks for new and existing employees), and technical (e.g. use of firewalls and intrusion detection systems to detect, restrict and monitor access to the systems and data/information - and secondary identification and authentication access controls).
- 24 Sr Official of Privacy Signature:

Abby Block
- 25 Sr Official of Privacy Signoff Date:

Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicare Financial Management & Payment Systems

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

2Summary of PIA Required Questions

Question	Response
1 System:	Medicare Financial Management & Payment Systems
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-01-06-02-1150-00 009-38-01-04-02-1105-00 009-38-01-09-01-1010-00
7 Privacy Act System of Records (SOR) Number:	09-70-0501, 09-70-0503
8 OMB Information Collection Approval Number:	N/A
9 Other Identifying Number(s):	CMS ART: OFM 463; PIMR: OFM 225
10 System Name:	Medicare Financial Management & Payment Systems
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	Antoinette Miller

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Medicare Financial Management & Payment Systems

12	Provide an overview of the system:	<p>Medicare Finance Management &amp; Payment System (MFMPs):</p> <p>CAFM: The CAFM system is the vehicle for tracking all benefit payments, banking issues, and CFO data.</p> <p>CAFMI: The CAFMI system is the main vehicle for planning, administering and monitoring the administrative expenses of the Medicare contractor community</p> <p>CAPTS: The CAPTS system will provide an efficient and effective method for tracking Corrective Action Plans related to audit findings as well as the most current status of those plans.</p> <p>CASR: The CASR System tracks budgeted and incurred costs for the Part A contractor audit and settlement functions by type of activity and type of provider or reporting entity.</p> <p>CERT: The CERT system produces national, contractor specific, and benefit category specific paid claim error rates.</p> <p>CMIS: The CMIS system monitors Medicare Fee-for-Service Contractor Performance.</p> <p>CMS ART: The CMS ART system provides cost and workload information on Program Safeguard Contractors (PSCs) and Qualified Independent Contractors (QICs)</p> <p>COB: The purpose of the COB Program is to identify the health benefits available to a Medicare beneficiary and involves the collection, management, and reporting of other insurance coverage.</p> <p>CROWD: The CROWD system provides CMS with a timely way to monitor each Medicare Contractor's performance in processing claims and paying bills.</p> <p>DPS: The DPS system provides payment data for issuance to demonstration providers and sites through the Financial Accounting Control System (FACS).</p> <p>HCRIS: The HCRIS system collects provider cost report information.</p> <p>PIMR: The PIMR system supports the tracking of Medicare fraud and abuse.</p> <p>PS&amp;R: The PS&amp;R system summarizes claims data information (statistical and payment data) for use in settling Medicare cost reports.</p> <p>PULSE: The PULSE system monitors Medicare Fee-for-Service contractor process counts.</p> <p>RAC: CMS has selected three states: California, Florida and New York, in which to conduct the Recovery Audit Contractors (RAC) demonstration project as required under Section 306 of the Medicare Modernization Act (1996). These three states were selected because they are among the states with the highest per capita Medicare services utilization rates. The RACs within these states will review hospital and other Part A claims, Part B claims, or DMERC claims from these states for the purpose of identifying overpayments and underpayments made by CMS. The RACs will review claims processed from FY2002 through the end of the demonstration project scheduled for FY2008.</p> <p>STAR: The STAR system is used by FIs to track the cost reporting process from due date to final settlement and the staff time associated with each task performed on a provider's cost report.</p>
----	------------------------------------	--

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Medicare Financial Management & Payment Systems

13	Indicate if the system is new or an existing one being modified:	Existing
14	Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	Yes
15	Is the system subject to the Privacy Act?	Yes
16	If the system shares or discloses IIF please specify with whom and for what purpose(s):	Yes: CAPTS: with the Administrator, COB: IRS and SSA. NO: CAFM, CAFMII, CASR, CERT, CMIS, CMS ART, CROWD, DPS, HCRIS, PIMR, PS&R, PULSE, RAC, STAR

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Medicare Financial Management & Payment Systems

- 17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:
- CAFM collects data on all benefit payments, banking issues, and CFO information from 40 input forms and to be used for analytical and monitoring purposes.
- CAFMII collects data from 11 input forms to accommodate new reporting requirements for the revised Medicare Contractor environment.
- CAPTS collects data on Corrective Action Plans to enable in the decision making process in helping to implement these plans.
- CASR data is collected from six input forms for monitoring purposes.
- CMIS collects monthly data from the Contractor Reporting of Operational and Workload Data (CROWD), the Medicare Contractor Process Counts Monitor System (PULSE) and the Contractor Administrative Financial Management System (CAFMII).
- CMS ART: Data is entered about contractor costs, workload and deliverables.
- COB: The purpose of the COB Program is to identify the health benefits available to a Medicare beneficiary and involves the collection, management, and reporting of other insurance coverage. as the sole COB contractor and maintainer of the COB System, GHI's Government Programs Division is responsible for ensuring the accuracy and timeliness of updates to Medicare's eligibility and entitlement databases, i.e., the Common Working File (CWF) and MEdicare Beneficiary Database (MBD) through the following tasks; Initial Enrollment Questionnaire (data on other insurance); IRS/SSA/CMS Data Match (information on whether or not a beneficiary or their spouse is working); Medicare Secondary Payer Claims Investigation (additional information related to the beneficiary's health benefit coverage); Coordination of Benefots Agreement (defines the criteria for transmitting enrollee eligibility data and Medicare adjudicated claim data to other insurers; Workman's Compensation Case Control (imaged copies of incoming cases); Voluntary Data Sharing Agreements to electronically exchange health insurance benefit entitlement; Medicare Prescription Drug Program Part D (collection and maintenance of prescription drug coverage data far Medicare Beneficiaries); National Call Center (trained staff charged with helping customers with COB questions.)
- CROWD: Data is collected from 30 input forms and is maintained on direct on-line storage for fiscal years 1986 through the current fiscal year.
- DPS: The system collects the minimally necessary identifying, medical and demographic information needed to reimburse demonstration providers for the services rendered to Medicare beneficiaries. The data collection is based on the individual demonstration legislation and only that information needed to pay correctly is collected.
- HCRIS: The information pertains to the providers' cost of doing business and various medical expenses.
- PIMR: PIMR collects, validates and consolidates on a monthly basis, operational and workload data from 70 Medicare contractors across the country as well as contractor administrative budget and financial management data from CMS systems into a single reporting system at CMS.
- PS&R: PS&R processes all Medicare Part A post-payment claims, breaking each claim into sub-claims based on fee and cost-based reporting criteria, then further summarizing the claims into an

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicare Financial Management & Payment Systems

aggregate amount per report type per provider. In order for the provider to reconcile its data and prepare for its cost report submission, it must be able to tie back the aggregated report amounts to the individual detail claims. The aggregated summary reports do not contain any sensitive information. It is only at the input paid claims and detail level that privacy-related information is present. The detail claims level is the minimum necessary to accomplish the purpose for the system, as, from an auditing and reimbursement perspective, the provider and intermediary must be able to tie summary totals back to the detailed claims records.

PULSE: On a nightly basis, Medicare contractors transmit their CMS-1565, CMS-1566, and CMS-1522 report files to the CMS data

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

CMS: Medicare Financial Management & Payment Systems

18 Describe the consent process:	<p>The CAFM, CAFMII, CASR and CROWD personal information is only accessed by the system administrator and the individual. Every system user must be registered and identified by their HDC User ID. The system administrator also enters their name. The first time a user accesses the system, he/she is prompted to enter their business address and phone number. Periodically, they are prompted to update this information.</p> <p>CAPT will obtain the information via mandated spreadsheets from the Medicare Contractor.</p> <p>CERT: Information is obtained directly from Medicare contractors' claims processing systems. Medicare beneficiaries sign a privacy act notice when they become eligible for Medicare that informs them that information they provide to justify payments will be used to determine the appropriate of payment.</p> <p>CMIS: There is no IIF data. CMS ART: There is no IIF data.</p> <p>COB: The purpose of the COB Program is to identify the health benefits available to a Medicare beneficiary and involves the collection, management, and reporting of other insurance coverage. As the sole COB contractor and maintainer of the COB System, GHI's Government Programs Division is responsible for ensuring the accuracy and timeliness of updates to Medicare's eligibility and entitlement databases, i.e., the Common Working File (CWF) and Medicare Beneficiary Database (MBD) through the following tasks: Initial Enrollment Questionnaire; IRS/SSA/CMS Data Match; Medicare Secondary Payer Claims Investigation; Coordination of Benefits Agreement; Workman's Compensation Case COntrol; Voluntary Data Sharing Agreements; Medicare Prescription Drug Program Part D; and National Call Center.</p> <p>DPS: The information is obtained electronically and hardcopy in a HIPAA compliant format. The suppliers of the information have been informed about data usage through either a contract or an informed consent form. These signed agreements are obtained as the supplier or beneficiary enters the demonstration.</p> <p>HCRIS: The Healthcare Cost Report Information System is an Oracle data base system containing cost report information from hospitals, SNFs, HHAs, hospice and renal providers. The reports are submitted by providers and updated on a daily flow basis.</p> <p>PS&amp;R: The information is present on the paid claims record, the format of which is specified by the FISS shared system. Claims, submitted by providers or billing houses, adjudicated by the Common Working File system, are placed into this paid claims format for input into PS&amp;R. This information is not shared with individuals nor is consent given for the data to be shared with individuals. The data is available to providers who provide services to Medicare beneficiaries, and is available to providers in summary and detail form.</p> <p>PULSE: Information is being collected from existing CMS reports here at CMS.</p> <p>RAC: There is no IIF data.</p> <p>STAR: The information in STAR does contain personally identifiable information within the STAR database about Medicare providers (employee names and TIN for providers). The STAR time keeping system lists name of FI employees and an employee number. These data are used only by the FI to track employees' time when the individual is working on a provider cost report. Employee data are not share by the FI or included in the National STAR database.</p>
----------------------------------	--

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Medicare Financial Management & Payment Systems

- 19 Does the system host a website?

Yes
- 20 Does the website have any information or pages directed at children under the age of thirteen?

No
- 21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?

Yes
- 22 Are there technical controls present?

Yes
- 23 Describe the IIF security controls:

COB: GHI has a Security Program that includes the CAST self-assessment with 441 administrative, physical and technical controls. The program includes security training, corrective action plans, Business Continuity Planning, external tests of security controls contracted to Cybertrust, SDLC, Change Control, Risk Assessments, System Security Plans. Full detail is available in the COB RA's, COB SSPs and COB BCP.
- 24 Sr Official of Privacy Signature:

Abby Block
- 25 Sr Official of Privacy Signoff Date:

Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicare Pricing Systems

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

2Summary of PIA Required Questions

Question	Response
1 System:	Medicare Pricing Systems
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-01-04-02-1105-00
7 Privacy Act System of Records (SOR) Number:	N/A
8 OMB Information Collection Approval Number:	N/A
9 Other Identifying Number(s):	N/A
10 System Name:	Medicare Pricing System
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	Daniel McGrane
12 Provide an overview of the system:	The systems that comprise the Medicare Pricing Systems Family provide software and data files to Medicare contractors and other entities for use in processing claims for Medicare covered services; provide reports for reconciliation of Medicare expenditures; and provide research capabilities in the form of lookup applications. Existing
13 Indicate if the system is new or an existing one being modified:	
14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	No
15 Is the system subject to the Privacy Act?	No
16 If the system shares or discloses IIF please specify with whom and for what purpose(s):	No
17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:	CMS will collect data from provider associations such as the American Medical Association, from workgroups of which CMS is a member and from data owned by CMS. The collected information is used to support policy decisions related to Medicare payment policies and to create systems appropriate to paying Medicare claims. The data collected is not personally identifiable information.
18 Describe the consent process:	No
19 Does the system host a website?	No
20 Does the website have any information or pages directed at children under the age of thirteen?	No
21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?	No
22 Are there technical controls present?	No
23 Describe the IIF security controls:	No
24 Sr Official of Privacy Signature:	Abby Block
25 Sr Official of Privacy Signoff Date:	Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Medicare Utilization Data Collection & Access Systems

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

2

### Summary of PIA Required Questions

Question	Response
1 System:	Medicare Utilization Data Collection & Access Systems
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-01-04-01-1160-00 009-38-02-00-01-1150-00 009-38-01-09-01-1010-00
7 Privacy Act System of Records (SOR) Number:	09-70-0558, 09-70-0514, 09-70-0571
8 OMB Information Collection Approval Number:	N/A
9 Other Identifying Number(s):	N/A
10 System Name:	Medicare Utilization Data Collection & Access System
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	Al Celentano

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



CMS: Medicare Utilization Data Collection & Access Systems

- 12 Provide an overview of the system:
- Data Extract System (DESY) – Enterprise Data Extract System for Enterprise Data

Data Agreement and Data Shipping (DADSS) – The Data Agreement and Data Shipping (DADSS) was created to provide an automated and easy-to-use system for tracking foreign media shipped from the CMS Data Center (CDC). DADSS provides data coordinators and CDC data release staff with the means to follow the movement of foreign media shipped from the CDC. This system maintains the accountability for the shipment of data from the CDC Tape Library.

HCIS/HCISMod (Health Care Information System/Health Care Information System Modernization) – HCIS/HCISMod is a multi-dimensional software application that provides an easy-to-use access path for non-programmers to manipulate Medicare data into information. HCIS provides Graphical User Interface (GUI) views and reports on the different types of Medicare services.

Incurred But Not Reported (IBNR) – The IBNR estimates represents the cost of services provided to Medicare beneficiaries but not paid at the end of the fiscal year, and is needed as part of the CMS financial statements.

Medicare Actuarial Data System (MADS) – The Medicare Actuarial Data Systems (MADS) incorporates monthly summarized Part A and quarterly summarized Part B data in relational statistical tables. The legislation authorizing this activity is OMB Circular A-130.

Monthly Bill and Payment Record Processing (MBPRP) – This system creates monthly and quarterly skeleton files that are used in a variety of other systems. Part A and Part B institutional claims data is used to create these skeleton files. Every input record processed has identifiable data but only select output files require identifiable data.

Medicare Provider Analysis and Review (MEDPAR) – The MEDPAR file is a representation of a beneficiary stay in an Inpatient hospital or Skilled Nursing Facility (SNF).

NCH Processing Reports (NCHPR) – The National Claims History Processing Reports detail by type of service the monthly and cumulative year-to-date totals of the number of claims processed and dollar amounts of adjudicated claims.

NCH Statistical Table System (NCHSTS) – This system produces various utilization tables of Medicare services.

NCH Summary (NCHSUM) – This system creates individual line item files for Medicare services and summarizes various pieces of information to feed to the Part B Extract and Summary System (BESS).

NCH Nearline Update and Maintenance System – The 100% Nearline File is the repository of all common working file (CWF) processed Part A and Part B detailed claims transaction records, beginning with service year 1991. The NCH contains both institutional claims processed by Fiscal Intermediaries (FI) and noninstitutional claims processed by local carriers and DMERCs.

National Medicare Utilization Database (NMUD) – NMUD is the new storage structure for the Medicare claims data. NMUD has been developed to replace the existing sequential flat files NCH with a DB2 environment as the enterprise Medicare utilization repository. NMUD will house CWF-processed detail claims transactions, beginning with service year 1998.

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicare Utilization Data Collection & Access Systems

	Integrated Data Repository- IDR is CMS' storage structure for detailed Medicare & Medicaid claims information
	APS- Retired
	BESS- Created to provide access to Part B claims information. Operates under TSO in the mainframe environment. Existing
13 Indicate if the system is new or an existing one being modified:	
14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	Yes
15 Is the system subject to the Privacy Act?	Yes
16 If the system shares or discloses IIF please specify with whom and for what purpose(s):	Data Extract System (DESY) – Other government agencies for fraud and abuse and disease management. Appropriate Data Use Agreement (DUA) is required. DADSS – Data Agreement and Data Shipping – N/A HCIS/HCISMod (Health Care Information System/Health Care Information System Modernization) – Other government agencies for fraud and abuse. Appropriate Data Use Agreement (DUA) is required. Incurred But Not Reported (IBNR) N/A Medicare Actuarial Data System (MADS) – N/A Monthly Bill and Payment Record Processing (MBPRP) – CMS staff/contractors Medicare Provider Analysis and Review (MEDPAR) – CMS Staff (including contractors) DESY DOJ OIG NIH Hospitals And Researchers. Consistent With CMS Mission Purposes, And With Required DUAs. NCH Processing Reports (NCHPR) – CMS staff/contractors NCH Statistical Table System (NCHSTS) – CMS staff/contractors NCH Summary (NCHSUM) – CMS staff/contractors NCH Nearline Update and Maintenance System – CMS staff/contractors; Federal and State agencies, researchers; hospitals, OIG, GAO and DOJ National Medicare Utilization Database (NMUD) – CMS staff/contractors; Federal and State agencies; researchers; hospitals, OIG, GAO, DOJ Integrated Data Repository (IDR)– CMS staff/contractors; Federal and state agencies; researchers; OIG, GAO, DOJ. APS - N/A. BESS - N/A.

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

CMS: Medicare Utilization Data Collection & Access Systems

- 17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:
- Data Extract System (DESY) – NCH and Enrollment information is disseminated via DESY. This data is used by government agencies to detect fraud and abuse and for disease management studies.

DADSS – Data Agreement and Data Shipping – DADSS data contains no Personal identifiers of any kind. It houses information related to legally binding Data Use Agreements and information used for shipping of data from the Data Center.

HCIS/HCISMod (Health Care Information System/Health Care Information System Modernization) – NCH, NMUD, Enrollment information is maintained in HCIS. This data is used by government agencies to detect fraud and abuse

Incurred But Not Reported (IBNR) – N/A

Medicare Actuarial Data System (MADS) – N/A

Monthly Bill and Payment Record Processing (MBPRP) – N/A

Medicare Provider Analysis and Review (MEDPAR) – NCH, or NMUDD Claim Information, with the included IFF, is used as inputs to the MEDPAR system to create a stay record, a representation of a beneficiary’s stay in an Inpatient Hospital or Skilled Nursing Facility (SNF)

NCH Processing Reports (NCHPR) – N/A

NCH Statistical Table System (NCHSTS) – N/A

NCH Summary (NCHSUM) – N/A

NCH Nearline Update and Maintenance System – N/A

National Medicare Utilization Database (NMUD) – N/A

Integrated Data Repository (IDR)– Claims information for CMS mission requirements

APS - Retired

BESS- Medicare Part B data

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: Medicare Utilization Data Collection & Access Systems

18	Describe the consent process:	Data Extract System (DESY) – PAD handles this.  DADSS – Data Agreement and Data Shipping – N/A  HCIS/HCISMod (Health Care Information System/Health Care Information System Modernization) – N/A  Incurred But Not Reported (IBNR) – N/A  Medicare Actuarial Data System (MADS) – N/A  Monthly Bill and Payment Record Processing (MBPRP) – N/A  Medicare Provider Analysis and Review (MEDPAR) – N/A  NCH Processing Reports (NCHPR) – N/A  NCH Statistical Table System (NCHSTS) – N/A  NCH Summary (NCHSUM) – N/A  NCH Nearline Update and Maintenance System – N/A  National Medicare Utilization Database (NMUD) – N/A  Integrated Data Repository (IDR)– N/A  APS- Retired  BESS- N/A
19	Does the system host a website?	Yes
20	Does the website have any information or pages directed at children under the age of thirteen?	No
21	Are there policies or guidelines in place with regard to the retention and destruction of IIF?	Yes
22	Are there technical controls present?	Yes
23	Describe the IIF security controls:	DESY-APCSS RUNS THIS SYSTEM IN THE DATA CENTER.  MEDPAR-APCSS RUNS THIS PRODUCTION SYSTEM IN THE DATA CENTER.  IDR is run in the data center.
24	Sr Official of Privacy Signature:	Abby Block
25	Sr Official of Privacy Signoff Date:	Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: Payment Quality Review Systems

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer "No" to that question.

2

Summary of PIA Required Questions

Question

Response

- 1 System:
- 2 Is this a new PIA?
- 3 If this is an existing PIA, please provide a reason for revision:
- 4 Date of this Submission:
- 5 OPDIV Name:
- 6 Unique Project Identifier (UPI) Number:
- 7 Privacy Act System of Records (SOR) Number:
- 8 OMB Information Collection Approval Number:
- 9 Other Identifying Number(s):
- 10 System Name:
- 11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:
- 12 Provide an overview of the system:

Payment Quality Review Systems

No

PIA Validation

Jun 29, 2007

CMS

009-38-01-09-01-1010-00

09-70-0534, 09-70-0527

0937-1012, 0938-0974, 0938-0994

FID-OFM-253

Payment Quality Review Systems

Lisa Beylis

PPRMS: PPRMS is a Congressionally mandated system that collects and analyzes physician/supplier and carrier claims data from the NCH SUM system in order to produce reports for trends analysis concerning physician access nationally.

PSOR: Tracks Part B overpayment and collections.

PORS: Tacks physician overpayment and collections.

REMAS: In most instances, Medicare is the primary payer for Medicare covered services furnished to Medicare beneficiaries. This means that Medicare's full authorized payment is made without considering any other insurance available to the Medicare beneficiary. In some instances where other insurance is available to pay for the furnished services and other conditions are satisfied, Medicare payment is secondary to the payment obligation of the other insurance. The applicable statute is 42 U.S.C. 1395y(b) and the applicable regulations are 42 C.F.R411 Subparts B-H. If Medicare makes a mistaken primary payment in such a situation, Medicare pursues recovery of the mistaken primary payment from an appropriate party. Appropriate parties include providers, suppliers, insurers, employers, beneficiaries and other applicable parties. Once identified, the mistaken primary payments are considered debts to the United States and accounted for on that basis in Medicare's accounting system and financial statements. ReMAS identifies instances where Medicare made a mistaken or conditional primary payment when it should have been the secondary payer. Claims are then identified and put into cases for the applicable debtor.

FID: The Fraud Investigation Database (FID) is a nationwide database directed to the accumulation of instances of potential and actual Medicare fraud and abuse cases, and the tracking of Medicare payment suspensions.

PERM: CMS has contracted with 3 federal contractors to identify error rates within the MEDicaid and SCHIP programs. These systems collect FFR claims, managed care payments, and eligibility information for both programs.

- 13 Indicate if the system is new or an existing one being modified:
- 14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?
- 15 Is the system subject to the Privacy Act?

Existing

Yes

Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Payment Quality Review Systems

- 16

If the system shares or discloses IIF please specify with whom and for what purpose(s):
- PPRMS: N/A

PSOR: The PSOR system shares data with the Debt Collection System.

ReMAS: Shares data with Debt Collection System, DOJ, Attorneys, OGC for the purpose of recovering monies due to the Trust Fund.

FID: Shares information with OIG/DHHS, DOJ, FBI, Medicaid PI directors, Medicare fraud control units

PURPOSE: To track specific case development and trends in Medicare fraud.

PERM: The 3 PERM contractors only share PERM data among themselves, as each is responsible for a piece of the entire PERM system. No other entity gets this data.
- 17

Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:
- PPRMS: The information analyzed is NCH SUM system RIC-M and RIC-O claims. The information is used to conducted detailed analyses on physician access and physician access trends in the US. Any data that is not necessary to this analysis is not saved for the output from the input SUM files. The data that is not used includes PII data.

PSOR: This system collects Part B overpayment at collection (i.e., recovery) information. A minimal level of data is collected due to privacy consideration.

REMAS: ReMAS collects identifying information (name, address, etc.) about beneficiaries that should have been covered under another insurance. Claim information for those beneficiaries is also collected so that users of ReMAS can identify whether each specific claim paid by Medicare was a mistaken or conditional payment that needs to be recouped. Identifying information (name, address, etc.) about providers and suppliers is also captured because that information is needed in order to develop a demand letter to the appropriate party.

FID: The agency accumulates information on cases of potential Medicare fee-for-service fraud and on payment suspensions.

PERM: CMS published a SOR for the 3 PERM system on May 16, 2006. The primary purpose of the PERM systems is to collect and maintain individually identifiable claims information in order to calculate payment error rates for the Medicaid and SCHIP programs. Information on Medicaid and SCHIP beneficiary eligibility from the annual random sample is also connected. Collection of this information has been identified as a "routine use" under the Privacy Act.

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



HHS Privacy Impact Assessment (PIA) Summary

CMS: Payment Quality Review Systems

- 18 Describe the consent process:

PPRMS: The information is obtained from the NCH SUM system. The administrators of this system are aware of this system's access through RACF permissions and profiles.

PSOR: Information is obtained from post-payment review and is collected from providers. It is conveyed by written demand letter.

REMAS: ReMAS has several electronic interfaces with other systems. Beneficiary data will be collected from the Medicare Beneficiary Database (MBD). Claims data will be collected from National Claims History (NCH) and National Medicare Utilization Database (NMUD) via the Data Extract System (DESY). Provider data will be obtained from the OSCAR, NSC and UPIN systems. Memorandums of Understanding between ReMAS and all other interfacing systems have been established.

FID: The FID information is entered by one of the following two groups: Medicare program safeguard contractors and Medicare Durable Medical Equipment Regional Carrier benefit integrity units. By it's nature, the subjects of potential fraud investigations are not generally advised that they are under scrutiny. The information itself is information that a Medicare carrier or intermediary would maintain on a provider or supplier that has billed the Medicare program for reimbursement, and includes all available identifying pieces of information given by that provider or supplier on their enrollment application and/or their bill or claim for payment. Information in the FID could also include summary of findings from Medical or other review of submitted and/or paid claims.

PERM: CMS collects only the information necessary to carry out its statutory mandate to estimate the amount of improper payments made in the MEDicaid and SCHIP programs. Per the PERM SOR, CMS will make disclosures from the PERM only with the consent of the subject individual, or his/her legal representative, or in accordance with the applicable exception provision of the Privacy Act. Information in the system is aquired either directly from the states or from Medicaid or SCHIP providers.
- 19 Does the system host a website?

Yes
- 20 Does the website have any information or pages directed at children under the age of thirteen?

No
- 21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?

Yes
- 22 Are there technical controls present?

Yes
- 23 Describe the IIF security controls:

Normal CMS Data Center physical security applies to all systems. Additionally:

PPRMS: Information is secured through RACF.

PSOR: ID and password are required to enter the system.

REMAS: The data in ReMAS will be secured through application security at the user level. Access to specific sets of data has also been set up at the database level.

FID: Users need a valid CMS user id and password to access the system. User ids and passwords are authenticated through CMS

PERM: IDs and Passwords are required to enter the system. Physical security measures and environment protection controls are in place, as well as System Rules of Behavior for contractor staff.
- 24 Sr Official of Privacy Signature:

Abby Block
- 25 Sr Official of Privacy Signoff Date:

Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



HHS Privacy Impact Assessment (PIA) Summary

CMS: Procurement & Property Management Systems

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

2

Summary of PIA Required Questions

Question

Response

- 1 System:
- 2 Is this a new PIA?
- 3 If this is an existing PIA, please provide a reason for revision:
- 4 Date of this Submission:
- 5 OPDIV Name:
- 6 Unique Project Identifier (UPI) Number:
- 7 Privacy Act System of Records (SOR) Number:
- 8 OMB Information Collection Approval Number:
- 9 Other Identifying Number(s):
- 10 System Name:
- 11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:
- 12 Provide an overview of the system:
- 13 Indicate if the system is new or an existing one being modified:
- 14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?
- 15 Is the system subject to the Privacy Act?
- 16 If the system shares or discloses IIF please specify with whom and for what purpose(s):

Procurement & Property Management Systems

No

PIA Validation

Jun 29, 2007

CMS

009-38-02-00-01-1150-00

09-70-3002, 09-70-0515, 09-70-0518

No

PRISM-OOM-223

Procurement and Property Management Systems

Brenda Pickering/Rod Bemson/Olen Clybourn

PPSM - The system tracks forms, manuals, publications, and commodities that are stored in the CMS warehouse. It maintains mailing lists, coordinates requests for printing services, distributes publications, and handles customer orders.

MMS - This COTS product is used for the storage and retrieval of publications, manuals, forms, and commodity items that are maintained in the CMS warehouse.

HOPS - The CMS Online Property System is an inventory and control system which tracks capitalized (cost \$25,000 or greater), accountable (cost between \$5,000 and \$24,999), and sensitive (cost less than \$5000) in-house and contractor property. HOPS tracks and reports on usage, depreciation, and disposal of this equipment.

PRISM – This COTS system tracks CMS contract and purchase order activity and produces documents and data for the FPDS-NG system.

RMS – The Records Management System (RMS) tracks the physical location of temporary Agency files stored in the Mezzanine level of the Centers for Medicare and Medicaid Services (CMS) Warehouse on a Kardex movable track filing system.

SUFS – The SiteMan Update File System exists to provide a data source for the Aperture space management software used by the OOM Administrative Services Group (ASG).

Existing

Yes

Yes

PRISM – Contractor/Vendor data is disclosed to the DHHS DCIS system, which then passes it on to the FPDS\_NG system. MMS - N/A. PPSM - N/A. HOPS - N/A. RMS - N/A.

The purpose is to comply with regulation on reporting of awarded contracts and purchase orders.

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



HHS Privacy Impact Assessment (PIA) Summary

CMS: Procurement & Property Management Systems

- 17

Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:
- CWOS - The business customer or CMS Inventory Specialist keys information into the CWOS system. Data includes business name, address, contact person, phone number, email address, publication number, and quantity requested.

HOPS - System information is collected from CMS procurement documents and personal property physical inventory activities. Information is used to track and account for CMS capitalized and accountable assets, and provide detailed records for capitalization depreciation schedules and property location assignments. This information is the minimum necessary to meet legal requirements for the control and management of government assets.

MMS - Information processed includes Inventory Control Number (ICN), warehouse location, customer number, item totals, and item quantities stored and picked.

PPSM – System information is collected from CMS procurement documents and customer order request forms. Information is used to monitor stock levels and locations, trigger stock reorder activities, stock order requests and customer ship-to information. Information processed includes Inventory Control Number (ICN), business customer information, item totals, and item quantities stored and picked.

RMS – Collects accession numbers, a CMS customers’ name-location-phone number-component, brief description of records stored, destroy date, number of boxes associated with each accession of record. The date collected is necessary in order to retrieve/return/dispose of records in storage.

SUFS - The agency will use information collected by the ASG Customer Service Team as part of the Administrative Services Group (ASG) move-order process.

PRISM - The information that is collected is voluntary information which is public information also contained in the federal CCR (Central Contractor Registry). This information is contained in the PRISM Vendor File. It included all information contained in SF 179. This data included vendor name, address, phone number, TIN, EIN, and DUNS numbers. The agency only used this data in order to mail documents to the vendor and to report to the Federal Procurement Data System (FPDS-NG).
- 18

Describe the consent process:
- SUFS – Having a very specific application, SUFS data disclosure and use will not change during the lifespan of the tool. As a result, notification of and consent to changes in practices are not necessary.

PRISM - Vendors can be contacted if necessary by way of generating mailing labels from the PRISM vendor file data. Any change in the use of this data would only be mandated by a change in federal statute or regulation.

SUFS - System does not directly collect IIF from individuals.

PRISM - Vendors can be contacted if necessary by way of generating mailing labels from the PRISM vendor file data. Any change in the use of this data would only be mandated by a change in federal statute or regulation.

PPSM - N/A

HOPS - N/A

MMS - N/A

RMS - N/A
- 19

Does the system host a website?
- Yes
- 20

Does the website have any information or pages directed at children under the age of thirteen?
- No
- 21

Are there policies or guidelines in place with regard to the retention and destruction of IIF?
- Yes
- 22

Are there technical controls present?
- Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Procurement & Property Management Systems

- 23 Describe the IIF security controls:

SUFS – The SUFS tool is available to a small user base, and IIF is secured using network authentication for tool access and database authentication for data access.  
PRISM - The PRISM system is available to a small user base (100 users), and IIF is secured using network authentication for tool access and database authentication for data access.  
PPSM - N/A  
HOPS - N/A  
MMS - N/A  
RMS - N/A  
Abby Block  
Jun 29, 2007
- 24 Sr Official of Privacy Signature:
- 25 Sr Official of Privacy Signoff Date:

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Provider Enrollment Systems

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

## 2 Summary of PIA Required Questions

Question	Response
1 System:	Provider Enrollment Systems
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-01-09-01-1110-00 009-38-01-09-01-1115-00 009-38-01-09-01-1010-00 009-38-01-04-01-1110-00
7 Privacy Act System of Records (SOR) Number:	09-70-0524, 09-70-0524, 09-70-0532, 09-70-0525, 09-70-0517, 09-70-0008, 09-70-0530
8 OMB Information Collection Approval Number:	PECOS: 0938-0685 (2/28/2004) UPIN: 0938-0685 (01/01/2007) MED: OFM 907
9 Other Identifying Number(s):	FMIB OFM-139 (NPPES) FMIB OFM-246 (PECOS) 500-02-0041 (MED) / Computer matching agreement between CMS and SSA for PECOS: CMA 2001-05
10 System Name:	Provider Enrollment Systems
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	Lisa Beylis, 410-786-6339

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: Provider Enrollment Systems

- 12 Provide an overview of the system:

NPDES: This initiative was mandated by the administrative simplification provisions of P.L. 104-191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA mandates the adoption of a standard health care provider identifier and its assignment to every health care provider that transacts electronically any of the transactions specified in that law.

MED: MED receives excluded provider data from OIG each month. The data is formatted and verified, and then distributed to all CMS contractors in accordance with sections 1128A & B and 1162(e) of the Social Security Act.

IRIS: IRIS is comprised of both a mainframe subsystem and a mid-tier subsystem called IRISV3. Teaching hospitals use IRISV3 to log the time worked by interns and residents at their hospitals. This data is tied to the hospitals cost report and is used as a determining factor on how much reimbursement the hospitals get in lieu of care given to Medicare and Medicaid patients. CMS collects the data and produces a periodic duplicate report which points out intrastate overlaps in periods worked by an intern or resident between two or more hospitals.

PECOS: The Medicare Federal Health Care Provider/Supplier Enrollment Application (CMS 855A, 855B, 855I, 855R, and 855S) has been designed by the Centers for Medicare and Medicaid Services (CMS) to assist in the administration of the Medicare program and to ensure that the Medicare program is in compliance with all regulatory requirements. The information collected in this application will be stored in the Provider Enrollment, Chain and Ownership System and used to ensure that payments made from the Medicare trust fund are only paid to qualified health care providers, and that the amounts of the payments are correct. The Centers for Medicare and Medicaid Services (CMS) is authorized to collect the information requested on this form by sections 1124(a)(1), 1124A(a)(3), 1128, 1814, 1815, 1833(e), and 1842(r) of the Social Security Act [42 U.S.C. §§ 1320a-3(a)(1), 1320a-7, 1395f, 1395g, 1395(l)(e), and 1395u(r)] and section 31001(1) of the Debt Collection Improvement Act [31 U.S.C. § 7701(c)]. The OMB approval number for this information collection is 0938-0685, and is renewed each time changes are made to the information collected.

PSCAS: HIPAA gave CMS authority to enter into contracts, consistent with the Federal Acquisition Regulations (FAR) to promote the integrity of the Medicare program. In May 1999, CMS awarded 13 PSC contracts to perform some, or all, of the program safeguard functions, i.e., medical review, benefit integrity, cost report audit, data analysis, MIP provider education. CMS has awarded more than 40 individual task orders under the PSC Umbrella contract. PSCs maintain claims and eligibility data for beneficiaries and providers in their service areas. The data is used for prevention and prosecution of Medicare fraud, waste and abuse.

NPICS: Data is extracted from NRRES and the provider files (PECOS) and compared to determine what Medicare legacy number and NPI should be mapped.
- Existing

13 Indicate if the system is new or an existing one being modified:

14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?

15 Is the system subject to the Privacy Act?

Yes

Yes

Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



# HHS Privacy Impact Assessment (PIA) Summary

## CMS: Provider Enrollment Systems

- 16

If the system shares or discloses IIF please specify with whom and for what purpose(s):
- CMS Staff, Other Federal Agencies, CMS contractors (IRIS)

Health plans as required by regulations, other federal agencies as described by SOR (NPPES)

NPPES will make all data (excluding the SSN and DOB) available in a downloadable file. This follows FOIA requirements. A file with DOB will only be available to those who have an approved DUA with CMS and only when the SSA and name of the provider is supplied and matchezs what is in NPPES.

Carriers, FI's, States, PSC's, and Medicare Advantage Players – to identify and refuse payment to excluded providers. (MED)

PSCAS: The system discloses information to DOJ and the OIG for HHS.

NPICS: Verify legacy/NPI pairs.
- 17

Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:
- NPPES: The system contains a unique identifier for each health care provider (the NPI, which is assigned by the NPS) along with other information about the provider. This information includes other identifiers, name(s), demographic, educational/professional data, and business address data. Only information required for establishing the identity of the health care provider will be collected. The information to be collected was issued in a Notice of Proposed Rulemaking in 1998, and unnecessary data was eliminated in response to comments.

MED: The only data taken from the OIG file is the data required to uniquely identify the provider in order to exclude the right guy (name, ssn, dob), as well as the pertinent exclusion data.

IRIS: Information is collected on 3½ inch floppy disks which are mailed to IRIS system maintainer. The information is used to create a periodic duplicate report and is released for research purposes. The minimum amount of data is collected to facilitate production of reports.

PECOS: The Medicare Federal Health Care Provider/Supplier Enrollment Application (CMS 855A, 855B, 855I, 855R, and 855S) has been designed by the Centers for Medicare and Medicaid Services (CMS) to assist in the administration of the Medicare program and to ensure that the Medicare program is in compliance with all regulatory requirements. The information collected in this application will be used to ensure that payments made from the Medicare trust fund are only paid to qualified health care providers, and that the amounts of the payments are correct. This information will also identify whether the provider is qualified to render health care services and/or furnish supplies to Medicare beneficiaries. To accomplish this, Medicare must know basic identifying and qualifying information about the health care provider that is seeking billing privileges in the Medicare program. Medicare needs to know: (1) the type of health care provider enrolling, (2) what qualifies this provider as a health care related provider of services and/or supplies, (3) where this provider intends to render these services and/or furnish supplies, and (4) those persons or entities with an ownership interest, or managerial control, as defined in this application, over the provider.

PSCAS: The system will maintain and disseminate Medicare claims history and MEDicare Provider characteristics to DOJ and OIG for the purposes of detecting, preventing, prosecuting Medicare fraud, waste and abuse.

NPICS: Data is extracted from NPPES and PECOS, NSC and NCPDP and compared tp determine what Medicare legacy number and NPI should be mapped.

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: Provider Enrollment Systems

18 Describe the consent process:	<p>NPPES: Information collected via the NPPES web site (internet) of paper application. Notification of NPI given via e-mail (if application was via web) or paper letter if application was via paper.</p> <p>MED: All our data and information comes from OIG. They provide us with a file, and Team MED pulls of the data we require to identify an excluded provider.</p> <p>IRIS: The information is obtained from Fiscal Intermediaries on 3 1/2 inch floppy disks who in turn receive the information from teaching hospitals.</p> <p>PECOS: The information will be collected from all health care providers and suppliers who render services or supplies to Medicare beneficiaries and bill the Medicare program for those services and supplies. This information will be collected via the completion of the CMS 855, Provider/Supplier Enrollment Application. All of this information is conveyed to the providers of the information in writing directly on the CMS 855 and in the certification signature page of the form.</p> <p>PSCAS: Individuals whose IIF is in the system when major changes occur to the system are notified through publication in the Federal Records of an update to the SOR for Medicare data.</p> <p>NPICS: Consent of individuals regarding IIF this system collects is obtained through the initial Medicare beneficiary agreement that is part of the application for Medicare benefits.</p>
19 Does the system host a website?	Yes
20 Does the website have any information or pages directed at children under the age of thirteen?	No
21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?	Yes
22 Are there technical controls present?	Yes
23 Describe the IIF security controls:	<p>NPPES: Users can get to their NPPES information via a valid user id and password. See the NPPES SSP for more information on system security.</p> <p>MED: The data is housed on the CMS mainframe, and is subject to standard CMS Data Center security policy.</p> <p>PECOS: Users need a valid CMS user id and password to access the system. User ids and passwords are authenticated through CMS.</p> <p>PSCAS: Federal Information Security Management Act requirements are implemented for this system including risk assessments, contingency plans, system security plans, and a self assessment.</p> <p>NPICS: The data is housed on the CMS mid-tier, and is subject to standard CMS Data Center security policy.</p>
24 Sr Official of Privacy Signature:	Abby Block
25 Sr Official of Privacy Signoff Date:	Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



HHS Privacy Impact Assessment (PIA) Summary

CMS: Q-Net

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

2Summary of PIA Required Questions

Question	Response
1 System:	Q-Net
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-01-06-01-1030-00
7 Privacy Act System of Records (SOR) Number:	N/A
8 OMB Information Collection Approval Number:	0938-0581 12/2007
9 Other Identifying Number(s):	N/A
10 System Name:	Q-Net
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	Dennis Stricker
12 Provide an overview of the system:	<p>QualityNet (QNet) is a General Support System (GSS). CMS maintains the QNet network infrastructure, a network environment that uses shared database servers and WAN/LAN resources to monitor and improve utilization and quality of care for Medicare and Medicaid beneficiaries. The program consists of the CMS Data Center Complex 1 located at the CMS central offices in Baltimore, MD; the alternate data center, known as Complex 2, located at the Iowa Foundation for Medical Care (IFMC) in Des Moines, IA; the Internet Complex, also known as Complex 3, located at Buccaneer Computer Systems &amp; Services, Inc. (BCSSI) in Warrenton, VA; a national network of 53 Quality Improvement Organization (QIO) sites responsible for each US state, territory, and the District of Columbia; 1 Clinical Data Abstraction Center (CDAC); 18 End Stage Renal Disease (ESRD) networks; and the two BCSSI and IFMC Contractor support locations.</p> <p>This legislation is under the Social Security Act, Title XVIII, Section 1864: “93.777 State Survey and Certification of Health Care Providers and Suppliers”</p> <p>This legislation is under Title XI of the Social Security Act, Part B, as amended by the Peer Review Improvement Act of 1982.</p> <p>This legislation is under Title XI--General Provisions, Peer Review, and Administrative Simplification</p> <p>The Balanced Budget Act of 1997 created section 1932 (c)(2) of the Act, which would replace section 1902 (a)(30)(C) with a new requirement for annual, external quality review (EQR) of Medicaid MCOs.</p>
13 Indicate if the system is new or an existing one being modified:	Existing
14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	Yes
15 Is the system subject to the Privacy Act?	Yes

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: Q-Net

16 If the system shares or discloses IIF please specify with whom and for what purpose(s):

The Quality Improvement System for Managed Care (QISMC) standards and guidelines are key tools for use by CMS and States in implementing the quality assurance provisions of the Balanced Budget Act of 1997 (BBA), as amended by the Balanced Budget Refinement Act of 1999. The QISMC standards and guidelines are intended to achieve four major goals:

- To clarify the responsibilities of CMS and the States in promoting quality as value-based purchasers of services for vulnerable populations.
- To promote opportunities for partnership among CMS and the States and other public and private entities involved in quality improvement efforts.
- To develop a coordinated Medicare and Medicaid quality oversight system that would reduce duplicate or conflicting efforts, and send a uniform message on quality to organizations and consumers.
- To make the most effective use of available quality measurement and improvement tools, while allowing sufficient flexibility to incorporate new developments in the rapidly advancing state of the art.

For further detailed information, please refer to the following Health Care Quality Improvement Systems (HCQIS) PIA's:  
Consolidated Renal Operations in a Web-Enabled Environment (CROWN)

Quality Improvement Evaluation System (QIES)

Standard Data Processing System (SDPS)

The QNet WAN/LAN network configuration provides the WAN/LAN connectivity and support for the Health Care Quality Improvement System that comprises of three Major Applications that collect information and operate within QNet network infrastructure:

- Standard Data Processing System (SDPS)
- Consolidated Renal Operations in a Web-Enabled Environment (CROWN)
- Quality Improvement Evaluation System (QIES)

The QNet WAN/LAN infrastructure supports the following CMS organizational business processes and data collection requirements:

- The capability for collection and management of clinical, survey, and project data from Medicare and Medicaid providers.
- The management and analysis of that clinical, survey, and project data with various SDPS programs by the Quality Improvement Organization (QIO).
- The collection of data by ESRD Network Organizations to administer the national Medicare ESRD program.
- The collection of provider and beneficiary-specific outcomes of care and performance data using QIES across a multitude of delivery sites (such as nursing homes and Rehabilitation and Long Term Care Hospitals, etc.) for use to improve the quality and cost effectiveness of services provided by the Medicare and Medicaid programs.
- The management and provision of Medicare and Medicaid information to providers that include but are not limited to Hospitals, physician or family practice clinics, dialysis clinics, Skilled Nursing Facilities, Home Health Agencies, and various specialized clinics.

For further detailed information, please refer to the following Health Care Quality Improvement Systems (HCQIS) PIA's:  
Consolidated Renal Operations in a Web-Enabled Environment (CROWN)

Quality Improvement Evaluation System (QIES)

Standard Data Processing System (SDPS)

17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

# HHS Privacy Impact Assessment (PIA) Summary

CMS: Q-Net

- 18 Describe the consent process:

For further detailed information, please refer to the following Health Care Quality Improvement Systems (HCQIS) Privacy Impact Assessments:  
Consolidated Renal Operations in a Web-Enabled Environment (CROWN)  
Quality Improvement Evaluation System (QIES)  
Standard Data Processing System (SDPS)
- 19 Does the system host a website?

Yes
- 20 Does the website have any information or pages directed at children under the age of thirteen?

No
- 21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?

Yes
- 22 Are there technical controls present?

Yes
- 23 Describe the IIF security controls:

For further detailed information, please refer to the following Health Care Quality Improvement Systems (HCQIS) Privacy Impact Assessments:  
Consolidated Renal Operations in a Web-Enabled Environment (CROWN)  
Quality Improvement Evaluation System (QIES)  
Standard Data Processing System (SDPS)
- 24 Sr Official of Privacy Signature:

Abby Block
- 25 Sr Official of Privacy Signoff Date:

Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

HHS Privacy Impact Assessment (PIA) Summary

CMS: Retiree Drug System (RDS)

1

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer "No" to that question.

2 Summary of PIA Required Questions

Question	Response
1 System:	Retiree Drug System (RDS)
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-01-04-01-1200-00
7 Privacy Act System of Records (SOR) Number:	09-70-0550
8 OMB Information Collection Approval Number:	0938-0957/0938-0977
9 Other Identifying Number(s):	FMIB # 6547
10 System Name:	Retiree Drug Subsidy System
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	Dave Gardner
12 Provide an overview of the system:	The RDS system is designed to provide information, enrollment, payment, and customer service for Plan Sponsors enrolled in the RDS Program. It is also designed to allow CMS to manage and track expenditures to Plan Sponsors as well as Plan eligibility and compliance.
13 Indicate if the system is new or an existing one being modified:	Existing
14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	Yes
15 Is the system subject to the Privacy Act?	Yes
16 If the system shares or discloses IIF please specify with whom and for what purpose(s):	RDS shares IIF with Federal Law Enforcement Agencies and with CMS information systems such as the MBD to verify retirees' ability to be claimed by an Employer Plan Sponsor as a qualifying covered retiree under the RDS program.
17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:	RDS collectes, maintains, and disseminates IIF with Federal Law Enforcement Agencies and with CMS internal systems such as the MBD to verify retirees' ability to be claimed by an Employer Plan Sponsor as a qualifying covered retiree under the RDS program.
18 Describe the consent process:	CMS is required to provide updated Notices of Privacy Practices .
19 Does the system host a website?	Yes
20 Does the website have any information or pages directed at children under the age of thirteen?	No
21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?	Yes
22 Are there technical controls present?	Yes
23 Describe the IIF security controls:	The data is maintained in the Data Zone of the RDS System and LDAP and other User Controls established to maintain control.
24 Sr Official of Privacy Signature:	Abby Block
25 Sr Official of Privacy Signoff Date:	Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.



HHS Privacy Impact Assessment (PIA) Summary

CMS: WAN Services MDCN	
------------------------	--

1	
---	--

The following required questions represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget. Note: If a question or its response is not applicable, please answer “No” to that question.

2	Summary of PIA Required Questions
---	-----------------------------------

Question	Response
1 System:	WAN Services MDCN
2 Is this a new PIA?	No
3 If this is an existing PIA, please provide a reason for revision:	PIA Validation
4 Date of this Submission:	Jun 29, 2007
5 OPDIV Name:	CMS
6 Unique Project Identifier (UPI) Number:	009-38-02-00-01-1150-00
7 Privacy Act System of Records (SOR) Number:	N/A
8 OMB Information Collection Approval Number:	N/A
9 Other Identifying Number(s):	N/A
10 System Name:	WAN Services/MDCN
11 System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	Charlene Fletcher
12 Provide an overview of the system:	This GSS provides compute platforms, telecommunications, electronic storage information and operations support services for the collection, maintenance, and access of data and information to support the business functions of CMS.
13 Indicate if the system is new or an existing one being modified:	Existing
14 Does/Will the system collect, maintain (store), disseminate and/or pass through IIF within any database(s), record(s), file(s) or website(s) hosted by this system?	No
15 Is the system subject to the Privacy Act?	No
16 If the system shares or discloses IIF please specify with whom and for what purpose(s):	No
17 Describe in detail the information the agency will collect, maintain, or disseminate and why and for what purpose the agency will use the information:	This GSS does not directly collect, maintain, or disseminate information. It provides platform support infrastructure for other CMS MA's to perform their function.
18 Describe the consent process:	No, this GSS does not directly collect, maintain, or disseminate information. It provides platform support infrastructure for other CMS MA's to perform their function.
19 Does the system host a website?	No
20 Does the website have any information or pages directed at children under the age of thirteen?	No
21 Are there policies or guidelines in place with regard to the retention and destruction of IIF?	No
22 Are there technical controls present?	No
23 Describe the IIF security controls:	The CMS WAN Services/MDN provides telecommunications infrastructure for use by other CMS business application Website functions, but does not directly provide a data or information content Website.
24 Sr Official of Privacy Signature:	Abby Block
25 Sr Official of Privacy Signoff Date:	Jun 29, 2007

Note on IIF: Any question about IIF seeks to identify any, and all, personal information associated with the system. This includes any IIF, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Note: If no IIF is contained in the system, please answer the remaining required questions, then promote the PIA to the Sr. Privacy Official who will authorize the PIA. Note: If this system contains IIF, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.